

Symantec™ Advanced Manager for Security Gateways (Group 1), Symantec™ Event Manager for Security Gateways (Group 1)

Integration Guide

Supported version: 2.0.1



Symantec Advanced Manager for Security Gateways, Symantec Event Manager for Security Gateways Integration Guide

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

PN: 10224090

March 10, 2004

Copyright notice

Copyright © 1998–2004 Symantec Corporation.

All Rights Reserved.

Any technical documentation that is made available by Symantec Corporation is the copyrighted work of Symantec Corporation and is owned by Symantec Corporation.

NO WARRANTY. The technical documentation is being delivered to you AS-IS and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained therein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Symantec reserves the right to make changes without prior notice.

No part of this publication may be copied without the express written permission of Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014.

Trademarks

Symantec, the Symantec logo, and Norton AntiVirus are U.S. registered trademarks of Symantec Corporation. LiveUpdate, LiveUpdate Administration Utility, Symantec AntiVirus, and Symantec Security Response are trademarks of Symantec Corporation.

Other brands and product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

Technical support

As part of Symantec Security Response, the Symantec global Technical Support group maintains support centers throughout the world. The Technical Support group's primary role is to respond to specific questions on product feature/function, installation, and configuration, as well as to author content for our Web-accessible Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering as well as Symantec Security Response to provide Alerting Services and Virus Definition Updates for virus outbreaks and security alerts.

Symantec technical support offerings include:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and Web support components that provide rapid response and up-to-the-minute information
- Upgrade insurance that delivers automatic software upgrade protection
- Content Updates for virus definitions and security signatures that ensure the highest level of protection
- Global support from Symantec Security Response experts, which is available 24 hours a day, 7 days a week worldwide in a variety of languages for those customers enrolled in the Platinum Support program
- Advanced features, such as the Symantec Alerting Service and Technical Account Manager role, offer enhanced response and proactive security support

Please visit our Web site for current information on Support Programs. The specific features available may vary based on the level of support purchased and the specific product that you are using.

Licensing and registration

This product requires a license file. The fastest and easiest way to register your service is to access the Symantec licensing and registration site at:

<https://licensing.symantec.com>.

See “Symantec Advanced Manager and Symantec Event Manager licensing” on page 155.

Contacting Technical Support

Customers with a current maintenance agreement may contact the Technical Support group by phone or online at www.symantec.com/techsupp/.

Customers with Platinum support agreements may contact Platinum Technical Support by the Platinum Web site at www-secure.symantec.com/platinum/.

When contacting the Technical Support group, please have the following:

- Product release level
- Hardware information
- Available memory, disk space, NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description
- Error messages/log files
- Troubleshooting performed prior to contacting Symantec
- Recent software configuration changes and/or network changes

Customer Service

To contact Enterprise Customer Service online, go to www.symantec.com/techsupp/, select the appropriate Global Site for your country, then select the enterprise Continue link. Customer Service is available to assist with the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information on product updates and upgrades
- Information on upgrade insurance and maintenance contracts
- Information on Symantec Value License Program
- Advice on Symantec's technical support options
- Nontechnical presales questions
- Missing or defective CD-ROMs or manuals

Contents

Section 1 Introducing Symantec Advanced Manager and Symantec Event Manager

Chapter 1 Introducing security gateway management with SESA

Managing security gateways through SESA	13
Products supported with Symantec Advanced Manager v2.0.1 and Symantec Event Manager v2.0.1	14
Symantec Advanced Manager for Security Gateways (Group 1) v2.0.1	15
Symantec Event Manager for Security Gateways (Group 1) v2.0.1	16
Where to get more information	18
Replacement CD-ROMs	18

Chapter 2 Understanding SESA management

About Symantec Enterprise Security Architecture	19
SESA components	19
SESA administrative features used with security gateways	21
Organizational units	21
SESA users	23
Roles in SESA	23
SESA event management features used with security gateways	24
Event logging and viewing	24
Alert and alert notifications	24
Centralized reporting	25

Chapter 3 Understanding advanced management

Advanced management concepts	27
Advanced management example	28
Security gateway configuration components in SESA	30
Configuration revisions	31
Associating policies and location settings with security gateways	31
Validating configurations	32
Activating configuration changes on security gateways	32

Advanced management of multiple security gateways	32
Multiple security gateway management example	33
Understanding how shared configurations are validated	36
Scalable management with organizational units	38
Organizational units	38

Chapter 4 Understanding event management

Event management concepts	41
Event management examples	42
Single security gateway example	42
Multiple security gateway example	43
SESA event gating	45
Viewing reports	46
Security gateway reports	46
Alerts and notifications	47

Chapter 5 Preparing to integrate security gateways with SESA

Planning for SESA integration	49
Analyzing your security needs	50
Required software	51
SESA Foundation Pack	51
Security gateways	51
Planning example	52
Choosing your starting point	54
Determining installation options and order	56
New installations	56
Upgrading from Symantec Advanced Manager	
for Security Gateways v2.0 and Symantec Event Manager	
for Security Gateways v2.0	57
Upgrading from Symantec Event Manager for Firewall v1.0	58

Section 2 Integrating Symantec security gateways with SESA

Chapter 6 Installing Symantec Advanced Manager for Security Gateways

About installing Symantec Advanced Manager	61
Symantec Advanced Manager for Security Gateways (Group 1) v 2.0.1	
installation CD-ROM contents	62
Before you install	63
Installing Symantec Advanced Manager for Security Gateways	64

Verifying the Symantec Advanced Manager installation	67
Upgrading from Symantec Advanced Manager for Security Gateways v2.0 to Symantec Advanced Manager for Security Gateways v2.0.1 ...	68
Upgrading from Symantec Event Manager for Security Gateways v2.0 to Symantec Advanced Manager for Security Gateways V2.0.1	68
Tuning Apache Tomcat memory usage on the SESA Manager	69
Increasing the memory used by the Apache Tomcat service	69
Lowering the memory usage values	70
Uninstalling Symantec Advanced Manager	71

Chapter 7 Installing Symantec Event Manager for Security Gateways

About installing Symantec Event Manager	73
Symantec Event Manager for Security Gateways (Group 1) v 2.0.1 installation CD-ROM contents	74
Before you install	75
Installing Symantec Event Manager for Security Gateways	76
Verifying the Symantec Event Manager installation	79
Upgrading from Symantec Event Manager for Security Gateways v2.0 to Symantec Event Manager for Security Gateways v2.0.1	80
Uninstalling Symantec Event Manager	80

Chapter 8 Joining security gateways to SESA

About joining SESA	83
Preparing to join SESA	84
Configuring the local security gateway	85
Joining multiple security gateways to SESA for centralized management	85
Joining SESA	86
Determining your options for joining SESA	87
Exporting the local security gateway configuration to SESA	88
Importing an existing policy and location settings from SESA	91
Joining a cluster to SESA	94
Joining SESA for event management only	99
Logging on to the SESA Console	100
Troubleshooting problems when joining SESA	100
Returning to local management	101

Section 3 Symantec Event Manager for Firewall (legacy products)

Chapter 9 Introducing Symantec Event Manager for Firewall (legacy products)

Using Symantec Event Manager for Firewall with legacy products and security gateways	108
How Symantec Event Manager for Firewall works	108
Symantec Event Manager for Firewall components	110
SESA integration components	110
How the Event Collector retrieves data	110
How the Event Collector works with the SESA Agent	111
How events are processed	111

Chapter 10 Remote Log utility

About the Remote Log utility	113
Enabling remote logging	114
Installing the Remote Log utility on the log server	116
Verifying remote logging operation	118

Chapter 11 Installing Symantec Event Manager for Firewall

About Symantec Event Manager for Firewall installation	120
Symantec Event Manager for Firewall components	120
System requirements and setup	123
SESA Foundation requirements	123
System requirements for the log server computer	124
Network sizing requirements for Symantec security gateways	125
Before you install	125
Installing SESA integration components on the SESA Manager	126
Installing Symantec Event Manager for Firewall components	
on the log server	127
Installing the Java Runtime Environment	127
Installing Symantec Event Manager for Firewall	128
Upgrading from Symantec Event Manager for Firewall v1.0	
to Symantec Event Manager for Security Gateways v2.0.1	134
Configuring network interfaces and remote management hosts	136
Customizing the SESA Agent's configuration	138
Customizing the SESA Manager's configuration	139

Configuring Symantec Event Manager for Firewall to monitor multiple Symantec Security Gateways	140
How the Event Collector for Symantec Security Gateways manages multiple log files	141
Configuring Symantec Event Manager for Firewall to monitor multiple log files	142
Event Collector for Symantec Security Gateways service/daemon	144
Starting and stopping the Event Collector in Microsoft Windows	144
Starting and stopping the Event Collector in Solaris	145
Managing disk space for log files	145
Archiving log files	145
Saving log files dynamically	146
Uninstalling the Event Collector for Symantec Security Gateways	147
Uninstalling the Event Collector in Microsoft Windows	147
Uninstalling the Event Collector in Solaris	147

Chapter 12 Verifying Symantec Event Manager for Firewall installation

Verifying that the service or daemon has started	149
Examining SESA Agent logs	150
Verifying Symantec Security Gateway appears in the SESA Console	151
Troubleshooting the Symantec Event Manager for Firewall installation	152
Verifying the SESA Manager address and port	153
Verifying remote logging operation for Symantec security gateways	153
Verifying Event Collector operation	154

Appendix A Licensing

Symantec Advanced Manager and Symantec Event Manager licensing	155
--	-----

Index

Introducing Symantec Advanced Manager and Symantec Event Manager

This section includes the following topics:

- [Introducing security gateway management with SESA](#)
- [Understanding SESA management](#)
- [Understanding advanced management](#)
- [Understanding event management](#)
- [Preparing to integrate security gateways with SESA](#)

Introducing security gateway management with SESA

This chapter includes the following topics:

- [Managing security gateways through SESA](#)
- [Products supported with Symantec Advanced Manager v2.0.1 and Symantec Event Manager v2.0.1](#)
- [Where to get more information](#)
- [Replacement CD-ROMs](#)

Managing security gateways through SESA

Symantec Advanced Manager for Security Gateways and Symantec Event Manager for Security Gateways are integrated with the Symantec Enterprise Security Architecture (SESA) to make it easier to manage your security gateways.

The Symantec Enterprise Security Architecture (SESA) provides a common framework that lets you integrate and manage multiple Symantec enterprise security and third-party products from a single, centralized location.

The SESA framework consists of a set of scalable, extensible, and secure technologies that make integrated security products interoperable and manageable, regardless of the size and complexity of your network.

When you manage your security gateways locally, you can only configure a single security gateway at a time or a cluster of identical security gateway machines.

When you use Symantec Advanced Manager to manage your security gateways through SESA, you can manage multiple security gateways. You can group them to reflect your organizational structure and create common configurations that can be shared by security gateways that have the same security postures.

The event management capabilities of Symantec Event Manager for Security Gateways, installed with Symantec Advanced Manager, give you up-to-date information you need to make informed decisions about the security of your network and related security gateways.

Products supported with Symantec Advanced Manager v2.0.1 and Symantec Event Manager v2.0.1

Symantec offers two SESA-enabled products that let you manage your security gateways through SESA. Each provides a different level of SESA management for Symantec security gateways and third-party products:

Table 1-1 How Symantec security gateways integrate with SESA

SESA Integration Products	Supported security gateways
Symantec Advanced Manager for Security Gateways (Group 1) v2.0.1	Policy Configuration: ■ Symantec Gateway Security 5400 Series v2.0 ■ Symantec Enterprise Firewall v8.0
	Event Management ■ Symantec Gateway Security 5400 Series v2.0 ■ Symantec Gateway Security 5110, 5200, 5300, 5310 v1.0* ■ Symantec VelociRaptor 500, 700, 1000, 1100, 1200, 1300, 1310 v1.5* ■ Symantec Enterprise Firewall v8.0 ■ Symantec Enterprise Firewall v7.0.x* ■ Select third-party products (via a separately purchased event collector)

Table 1-1 How Symantec security gateways integrate with SESA (Continued)

SESA Integration Products	Supported security gateways
Symantec Event Manager for Security Gateways (Group 1) v2.0.1	Symantec Gateway Security 5400 Series v2.0
	Symantec Gateway Security 5110, 5200, 5300, 5310 v1.0*
	Symantec VelociRaptor 500, 700, 1000, 1100, 1200, 1300, 1310 v1.5*
	Symantec Enterprise Firewall v8.0
	Symantec Enterprise Firewall v7.0.x*
	Select third-party products (via a separately purchased event collector)

* The Symantec security products that are marked with an asterisk do not have integrated SESA support.

To view events for these products in SESA, you must install the Symantec Event Collector for Security Gateways and SESA Agent.You install these components on the log server that collects your legacy Symantec security gateways events. These components are included on your product CD-ROM.

See *“Installing Symantec Event Manager for Firewall” on page 119.*

Note: Symantec Advanced Manager and Symantec Event Manager require SESA Foundation Pack v1.1.5 (purchased separately).

You must install your SESA environment and ensure that it is fully operational before you install the Symantec Advanced Manager or Symantec Event Manager on the SESA Manager computer.

Consult the *Symantec Enterprise Security Architecture Installation Guide* and the *Symantec Enterprise Security Architecture Administrator’s Guide* for further information.

Symantec Advanced Manager for Security Gateways (Group 1) v2.0.1

You install the Symantec Advanced Manager for Security Gateways software on your SESA Manager computer. This lets you access your security gateway configurations and events through the SESA Console, a Web-based graphical user interface. From the SESA Console, you can monitor and organize a large number of security gateways, along with other supported SESA products.

Advanced management through SESA lets you manage both policies and location settings of connected security gateways, in addition to collecting events from those systems. Symantec Advanced Manager also provides scalable

management by allowing multiple security gateways to share common policies and location settings.

Symantec Advanced Manager provides many features important to centralized and scalable management, including:

- Logical grouping of security gateways into organizational units
- Management of multiple configurations
- Sharing of configurations across security gateways
- Validation of multiple configurations in a single action
- Distribution of configurations to many security gateways in a single action

The Symantec Advanced Manager also includes the Symantec Event Manager for Security Gateways (Group 1) v2.0.1 (described in the next section) for centralized event logging, alerting and reporting.

Symantec Event Manager for Security Gateways (Group 1) v2.0.1

The Symantec Event Manager for Security Gateways is a standards-based software security solution that provides centralized logging, alerting, and reporting across Symantec's security gateway protection solutions and third-party products (purchased separately).

The Symantec Event Manager is automatically installed if you install the Symantec Advanced Manager for Security Gateways.

If you simply want to manage events from your security gateways, you can install only the Symantec Event Manager for Security Gateways on the SESA Manager computer. Then you use the Security Gateway Management Interface (SGMI) on your local machine to join SESA for event management only.

The Symantec Event Manager collects information from security gateways that have joined SESA and reports events to the SESA Console, letting you see security events and log messages in a tabular or graphical format. You can view event reports for any security gateway that has joined SESA.

The advantage of event management through SESA is that instead of having to go to each system, generate a usage report, and then manually cross check this report against reports from all other products, you can perform this task once, at one location, and collect reported events for all of your managed products.

By collecting and formatting information from Symantec and third-party supported products, the Symantec Event Manager for Security Gateways can consolidate and normalize security gateway event data, making impending threats more easily identifiable.

Combining powerful alert notification, enterprise reporting and role-based administration with a highly scalable secure architecture, the Symantec Event Manager for Security Gateways is ideally suited for medium-to-large enterprises and supported security services environments.

If you have separately purchased an Event Collector for a third-party firewall product, you can also view events generated by that product.

Symantec Event Manager for Firewall v1.0

Symantec Event Manager for Firewall v1.0 is included on the Symantec Advanced Manager for Security Gateways and Symantec Event Manager for Security Gateways CD-ROMs. Symantec Event Manager for Firewall integrates event collection for legacy Symantec security gateways and third-party security gateways with Symantec Enterprise Security Architecture (SESA) v1.1.5.

See [Table 1-1, “How Symantec security gateways integrate with SESA,”](#) on page 14.

The Symantec Event Manager for Firewall delivers enterprise firewall security information to a central SESA DataStore, allowing you to use the SESA Console to see a consistent view of your firewall security events.

Event reporting to SESA

Symantec security gateways such as Symantec Gateway Security 5400 Series appliances and Symantec Enterprise Firewall v8.0, and Symantec legacy products use different processes to report events to SESA:

- When a Symantec Gateway Security 5400 Series appliance or Symantec Enterprise Firewall v8.0 joins SESA, a SESA Agent is downloaded to the security gateway and activated. This SESA Agent formats event messages, making them acceptable to SESA, and then forwards the events to the SESA Manager.
- Legacy Symantec security gateway products use an intermediate log server to collect events.

See [Table 1-1, “How Symantec security gateways integrate with SESA,”](#) on page 14.

You install the SESA Agent on the log server. It then formats messages that are sent to the log server, making them acceptable to SESA, and forwards the events to the SESA Manager.

Note: For more information on managing Symantec legacy products from SESA, see [“Introducing Symantec Event Manager for Firewall \(legacy products\)”](#) on page 107.

Where to get more information

This guide is intended for administrators who will install the SESA integration components for one of the following products:

- Symantec Advanced Manager for Security Gateways (Group 1) v2.0.1
- Symantec Event Manager for Security Gateways (Group 1) v2.0.1

This guide describes how to join the security gateway to SESA. You can find additional information in supporting documents that are provided in PDF format on the product software CD-ROMs.

The following documents are provided on the product CD-ROMs:

- *Symantec Advanced Manager for Security Gateways (Group 1) v2.0.1 and Symantec Event Manager for Security Gateways (Group 1) v2.0.1 Administrator's Guide*
- *Symantec Advanced Manager for Security Gateways (Group 1) v2.0.1 and Symantec Event Manager for Security Gateways (Group 1) v2.0.1 Release Notes*

This guide assumes that your SESA environment is already installed and working properly. If your SESA environment is not yet installed, consult the *Symantec Enterprise Security Architecture Installation Guide* and the *Symantec Enterprise Security Architecture Administrator's Guide*.

Replacement CD-ROMs

You may need to replace the media due to a defective or lost CD-ROM. If you need a replacement CD-ROM because it is defective, email supportsolutions@symantec.com.

If you require a new CD-ROM because you have lost it, contact your Sales Representative or reseller to purchase a new media kit.

Understanding SESA management

This chapter includes the following topics:

- [About Symantec Enterprise Security Architecture](#)
- [SESA administrative features used with security gateways](#)
- [SESA event management features used with security gateways](#)

About Symantec Enterprise Security Architecture

Symantec Enterprise Security Architecture (SESA) integrates multiple Symantec enterprise security products and third-party products to provide flexible control of security within organizations. SESA provides a common management framework, known as the SESA foundation, for the SESA-enabled security products that protect your IT infrastructure.

The SESA Console is the common user interface that provides manageable integration of your security technologies (Symantec or otherwise).

For detailed information about SESA, see the *Symantec Enterprise Security Architecture Installation Guide* and the *Symantec Enterprise Security Architecture Administrator's Guide*.

SESA components

The SESA foundation consists of several individual components that together provide a unique, scalable security infrastructure.

SESA uses SESA Agents that are installed on security product, a SESA Directory, a SESA DataStore, and a SESA Manager to collect, store, process, and report security events to the SESA Console, and to distribute configuration changes to SESA and SESA-enabled security products. In some cases, security products may

also use a SESA Event Collector to collect security events for forwarding to SESA.

[Table 2-1](#) describes how the security gateway integrates with the individual SESA components.

Table 2-1 Symantec security gateway relationship to SESA

SESA Component	How the security gateway interacts
SESA Manager	The SESA Manager is the hub for the SESA Directory and the SESA DataStore. It is a central processing unit (server) for the SESA Agents, SESA DataStore, SESA Directory, and SESA Console. All SESA data passes through the SESA Manager. You install Symantec Advanced Manager for Security Gateways and Symantec Event Manager for Security Gateways on the SESA Manager computer.
SESA DataStore	This relational database stores all event and alert data generated by SESA and SESA-enabled products such as Symantec security gateways.
SESA Directory	The SESA Directory stores the configuration data required to manage SESA-enabled security products and SESA services on the network. As new security gateways are installed, SESA automatically adds the devices to the SESA Directory.
SESA Agent	The SESA Agent runs on the security gateway and handles communications between the SESA-enabled security gateway and the SESA Manager. It passes data from the security gateway to the SESA Manager and receives product configuration data. For legacy Symantec security gateways and third-party security gateways, the SESA Agent works with installed event collectors to pass event data to the SESA Manager. For more information on managing Symantec legacy or third-party products from SESA, see “Introducing Symantec Event Manager for Firewall (legacy products)” on page 107.
SESA Console	The SESA Console is a Java-based framework that creates a common environment for the management of diverse security products. It runs in a Web browser with a secure connection and provides the graphical user interface that you use to view events and to push down configurations. With Symantec Advanced Manager, you use the SESA Console to view, manage, and distribute security gateway configurations, as well as view events. With Symantec Event Manager, you use the SESA Console to view and analyze events.

SESA administrative features used with security gateways

To manage your security gateways in SESA, you must plan for and configure some of SESA's administrative features. You perform these tasks from the SESA Console System view tab, using SESA wizards.

Features that you will configure include:

- Organizational units that reflect the organization of your security gateways
- Users who will use SESA to manage or monitor security gateways
- Roles that define what users can see and do in the SESA Console

Note: The SESA System view tab also lets you create configuration groups to distribute configurations that supersede those distributed by organizational units.

While you can use this method to distribute configurations for other security products, you cannot use configuration groups to distribute Symantec security gateway configurations.

Organizational units

Organizational units let you define the top level organization of your security gateways so that your SESA environment reflects how your organization is handling or plans to handle its security management needs.

You can create organizational units based on any of the following:

- Business functions, such as marketing, operations, and accounts payable
- IT functions
- Product groups, such as antivirus and firewall
- Location; for example: regions, cities, or building floors
- A combination of location and business function

Note: For Symantec Advanced Manager you must create organizational units at a single level. For other products and other uses of SESA you can create organizational units using a hierarchical structure to reflect your organization's management structure.

SESA uses organizational units to contain the computers on which SESA-enabled products are installed. When you run the Join SESA Wizard, you place your security gateway machine in an organizational unit and register it with SESA.

If you have already created organizational units in SESA, when you run the Join SESA wizard, you can specify the organizational unit to which your security gateway machine will belong. If you have not created organizational units, you can place your security gateway machines in either the Default or Managers organizational unit when you join them to SESA.

You can use organizational units to deploy your security gateway configurations to groups of security gateways in your network. If you associate a configuration directly with an organizational unit, each computer and appliance that you assign to the organizational unit inherits the configuration.

For example, when a security gateway that is a member of a cluster joins SESA, it and all other members of the cluster are placed in a single organizational unit. All cluster members inherit their configurations from the configuration that is associated with the organizational unit.

Default organizational units

The organizational units in [Table 2-2](#) already exist when you access the SESA Console for the first time.

Table 2-2 Default organizational units

Organizational unit	Description
Default	The Default organizational unit contains computers on which SESA Agents are installed, but have not yet been assigned to other organizational units. When you create organizational units, you can move computers from the Default unit to a newly created organizational unit as necessary.
Managers	The Managers unit contains computers on which the SESA Manager is installed. You cannot move computers that have SESA Managers installed on them from the Managers unit to other organizational units: SESA Managers always stay in the Managers organizational unit. When a SESA Manager computer also has a SESA-enabled security product installed, the computer remains in the Managers unit and does not show in the Default unit or any other unit.

SESA users

SESA maintains a list of SESA users, who are people who have SESA management or non-management roles.

A Default Administrator user is defined during SESA installation. The Default Administrator has access rights to the entire SESA administrative domain. When you first log on to the SESA Console, it will be as the Default Administrator.

For ongoing use, you should determine how your SESA environment will be accessed. Your choices include:

- A single administrator
- Multiple administrators, each managing a separate security product
- Users whose purpose in accessing SESA is only event monitoring
- Users who will be the recipients of notifications

If you do not plan to have a single administrator, you should create SESA users for each type of SESA access you require.

When you create SESA users, they have no access rights. For users to log on to the SESA Console, you must give them permissions appropriate to their management responsibilities. These permissions are defined in SESA roles that you create and assign to users. See [“Roles in SESA”](#) on page 23.

Roles in SESA

SESA uses role-based administration. A role is a set of permissions for specific management operations. A SESA Console user can be a member of one or more roles. The logon identity of SESA Console users determines their role assignment during an administrative session.

Roles separate permissions for accessing and using SESA. Roles that you can create for security gateway management in SESA include:

- Event management roles
You can assign administrators who monitor events and alerts to a Security Monitoring role. When they log on to SESA, this role lets them view data from all types of SESA-enabled security products, but does not grant permission to change product configurations.
- Configuration management roles
You can give your security gateway administrators role assignments that allow them to change and distribute configurations but not to view events from other security products.

- The SESA Domain Administrator role
SESA installs with a SESA Domain Administrator role, which is assigned to the Default Administrator user. The Domain Administrator role includes permissions to add users, roles, organizational units, and configuration groups to the SESA domain.
SESA users who do not belong to the SESA Domain Administrator role cannot see the System view tab in the SESA Console. You can add users to the Domain Administrator role to grant Domain Administrator Role permissions and access to the System view tab.

SESA event management features used with security gateways

SESA helps organizations manage security events by providing common logging of normalized event data for SESA-supported and SESA-enabled security products. In addition, SESA has a notification system for the events that are generated by SESA-enabled security products and SESA itself. SESA also provides robust reporting capabilities.

Event logging and viewing

SESA provides centralized logging and event viewing capabilities. Each Symantec security gateway forwards events to its SESA Agent, which manages and queues the events and sends them to a SESA Manager. The SESA Manager then logs the events in the SESA DataStore.

Event viewing is provided through the SESA Console Events view tab. You can query, filter, and sort events to quickly find computers that are not protected, have out-of-date configurations, or have high-severity events occurring on them.

Alert and alert notifications

SESA lets you create alert configurations for events that are collected in the SESA DataStore.

You can configure alerts to use a specific set of event criteria. You can also specify that an alert will accumulate events until a certain number are received or within a time interval. By specifying event criteria and applying thresholds, you can use alerts to consolidate the many events that SESA-enabled security products generate.

Alert configurations can also include notifications to pagers, SNMP traps, email, and operating system event logs. You can define the notification recipients, day and time ranges when specific recipients are notified, and custom data to accompany the notification messages. Each notification recipient has one or more preferred ways of receiving notification. You choose the user to notify for a particular alert or group of alerts.

Centralized reporting

SESA provides centralized reporting capabilities, including graphical reports. SESA installs with some common reports. Security gateways have additional predefined reports. You can also create custom reports.

You can use reports to present statistics, recent activity, outbreak and intrusion conditions, and so on. SESA provides a variety of report formats such as trend graphs, pie charts, stacked bar charts, and tables, all of which let you drill down to the particular data that you need. You can print current SESA Console views of events and alerts as reports, or save the views as reports and export them to other formats.

Understanding advanced management

This chapter includes the following topics:

- [Advanced management concepts](#)
- [Advanced management of multiple security gateways](#)
- [Scalable management with organizational units](#)

Advanced management concepts

The Symantec Advanced Manager gives you advantages over management from a local security gateway.

With Symantec Advanced Manager, security gateway management is:

- **Centralized**
You can manage multiple security gateways from a single SESA Console by modifying security gateway configurations in SESA and then deploying them to individual computers.
- **Scalable**
The Symantec Advanced Manager lets you manage multiple gateways together, with less effort than it would take to manage them individually by deploying a single configuration to a group of security gateways.
- **Integrated**
Integration with SESA lets you manage multiple SESA-enabled products together, with less effort than it would take to manage them individually.

To understand how Symantec Advanced Manager lets you manage security gateways through SESA, you should become familiar with some advanced management concepts.

These advanced management concepts include:

- How the components of a security gateway configuration are created and used in SESA.
See [“Security gateway configuration components in SESA”](#) on page 30.
- How Symantec Advanced Manager handles configuration revisions.
See [“Configuration revisions”](#) on page 31.
- How configurations are associated, validated, and activated for your security gateways.
See [“Associating policies and location settings with security gateways”](#) on page 31, [“Validating configurations”](#) on page 32 and [“Activating configuration changes on security gateways”](#) on page 32.

Advanced management example

To understand how you can use Symantec Advanced Manager to manage policies and location settings, consider the example of a single managed security gateway.

[Figure 3-1](#) shows a network with a Symantec Enterprise Firewall (2) that is managed using Symantec Advanced Manager. This network also has three Symantec Gateway Security appliances from which events are collected.

You can easily manage mixed environments, where some systems are joined for event management only, and others are joined for advanced management.

Figure 3-1 Simple centralized management

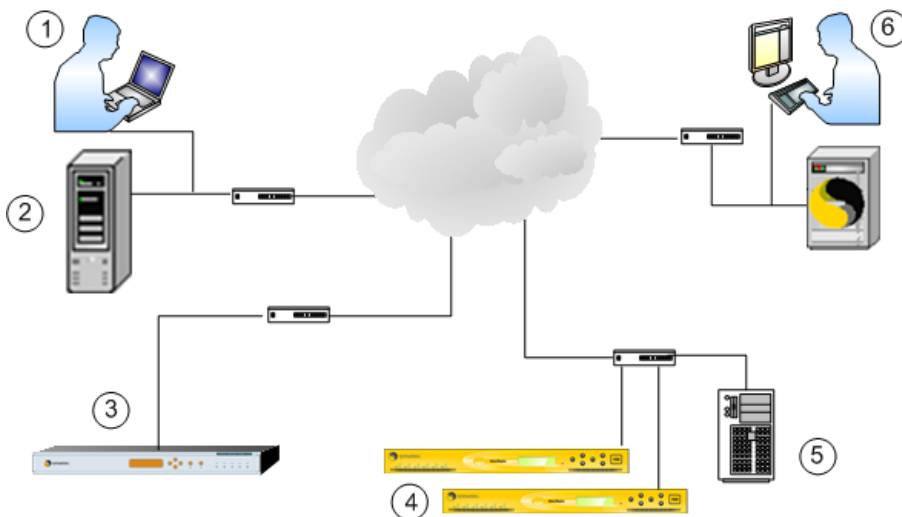


Table 3-1 describes the components in Figure 3-1.

Table 3-1 Descriptions of components in Figure 3-1

Callout	Description
1	Security Gateway Management Interface (SGMI)
2	Symantec Enterprise Firewall V8.0 Joined to SESA for advanced management.
3	Symantec Gateway Security 5420 appliance v2.0. Joined to SESA for event management only.
4	Symantec Gateway Security appliances v1.0 Joined to SESA for event management only, by way of the log server.
5	Symantec Event Manager for Firewall Log Server. You install the Symantec Event Collector for Security Gateways and the SESA Agent on this system to collect events from legacy systems, and then forward them to the SESA Manager.
6	SESA Console and SESA Manager.

For the easiest transition to managing security gateways by using Symantec Advanced Manager, you should begin by configuring a policy and location settings on your local security gateway.

When you join the security gateway to SESA, export the policy and location settings that you created locally, so that they are stored in SESA. (See [“Choosing your starting point”](#) on page 54.)

After you join SESA, when you log on to the SESA Console, the policies and location settings are available for you to modify. You can change either the policy or the location settings, and then validate and activate your changes on the security gateway.

Security gateway configuration components in SESA

You manage SESA-enabled security gateways by creating and distributing security gateway configurations that are stored in SESA.

A security gateway's configuration is a combination of the following:

- A policy and location settings
You configure policy and location settings in SESA in the same way as you configure them in the Security Gateway Management Interface (SGMI). The difference is that in SESA you can configure policy or location settings once and then apply them to multiple security gateways.
- System-specific settings that are specific to the local gateway
When the security gateway joins SESA, the system information about the physical machine is sent to SESA.

When you join a security gateway to SESA, you can export and register a copy of the security gateway's local configuration with SESA, or you can inherit a previously registered configuration. SESA stores the associated policy and location settings for each registered system.

Policies

A policy describes the security stance of the security gateway to which it is applied. Using Symantec Advanced Manager, you can share policies among multiple security gateways.

The policies you define using the SESA Console are identical to the policies you define by way of the Security Gateway Management Interface (SGMI). They contain data such as firewall rules, service groups, VPN policies, and content filtering.

For Symantec Gateway Security appliances, you can also apply antivirus, intrusion detection, and intrusion prevention policies.

Location Settings

Location settings describe the network in which a security gateway lives by grouping logical network and user definitions. They include definitions of network entities, tunnels, and users.

Locations settings can be shared among multiple security gateways, but are often uniquely defined for each specific location in which a single or clustered Symantec security gateway environment exists.

As with policies, the location setting options that you configure using Symantec Advanced Manager are identical to those that you configure in the Location Settings window of the SGMI.

Local system settings

Each security gateway that connects to SESA has some settings that apply only to that system. System settings are configured locally through SGMI, and are not configured using the SESA Console.

Local system settings include local system information, network interfaces and routes, license features, and cluster configurations.

Before you distribute a configuration, Symantec Advanced Manager validates it against the stored copy of your local system settings.

Configuration revisions

A revision is a version of a configuration. As you modify a configuration's policy or location settings, and deploy these modifications, a new revision is created.

Only two revisions are maintained by Symantec Advanced Manager for Security Gateways at any given time: the revision that has been distributed (currently active), and a working copy that may not yet have been validated and activated.

When you make changes to a configuration, you can copy the current configuration and work with the copy instead of working with the active configuration.

To learn how to copy or delete a configuration, see the section on Symantec Advanced Manager configuration commands in the *Symantec Advanced Manager for Security Gateways (Group 1) v2.0.1* and *Symantec Event Manager for Security Gateways (Group 1) v2.0.1 Administrator's Guide*.

Associating policies and location settings with security gateways

Every security gateway that is managed by Symantec Advanced Manager is configured with a policy and location settings. For the security gateway to function properly, the policy and location settings must function properly with each other.

To ensure this, Symantec Advanced Manager validates the policy and location settings against each other, and against the local system settings before they are activated on a security gateway. Before the validation can take place, you must associate the policy and location settings with a security gateway, so that Symantec Advanced Manager knows which local system settings to use when validating.

To determine which security gateways you will impact if you make a change to a selected policy or location settings, you can use the Symantec Advanced Manager Show all associated gateways feature to display all the security gateways that are associated with the policy or location settings.

For more information, see the section on associating policies and location settings with security gateways in the *Symantec Advanced Manager for Security Gateways (Group 1) V2.0.1* and *Symantec Event Manager for Security Gateways (Group 1) V2.0.1 Administrator's Guide*.

Validating configurations

Validation is the process that checks a configuration for completeness, ensures that all values are valid, and determines if all logical and physical references between a policy, location settings, and a security gateway's system settings can be resolved. Symantec Advanced Manager for Security Gateways uses validation to ensure that each connected security gateway gets a policy and location settings that work for that system.

To learn how to run the Validation Wizard, see the section on validating policy or location settings in the *Symantec Advanced Manager for Security Gateways (Group 1) V2.0.1* and *Symantec Event Manager for Security Gateways (Group 1) V2.0.1 Administrator's Guide*.

Activating configuration changes on security gateways

Activation is the process that Symantec Advanced Manager for Security Gateways uses to push a new version of a configuration down to all security gateways that use it.

Successful validation is a required piece of the activation process. When you select Activate from the Selection menu, SESA first validates the configuration, and then, if validation is successful, activates the changes.

To learn how to activate a configuration, see the section on activating policy or location settings in the *Symantec Advanced Manager for Security Gateways (Group 1) V2.0.1* and *Symantec Event Manager for Security Gateways (Group 1) V2.0.1 Administrator's Guide*.

Advanced management of multiple security gateways

The fundamental concepts that apply to managing a single system also apply to managing multiple security gateways.

Symantec Advanced Manager provides additional capabilities that let you organize your security gateways into logical groupings, and apply the same policies to similar security gateways. As you add new security gateways, you can

use the policies that you have already created to quickly provide them with configurations.

When you manage multiple security gateways, you can use SESA organizational units to group your security gateways in the SESA Console System view. This lets you more clearly see how the entire network is structured. Organizational units also provide a mechanism to let member security gateways inherit an associated policy and location settings, simplifying management of many systems.

Multiple security gateway management example

[Figure 3-2](#) shows multiple security gateways, most of which have joined SESA for advanced management.

Figure 3-2 Scalable management

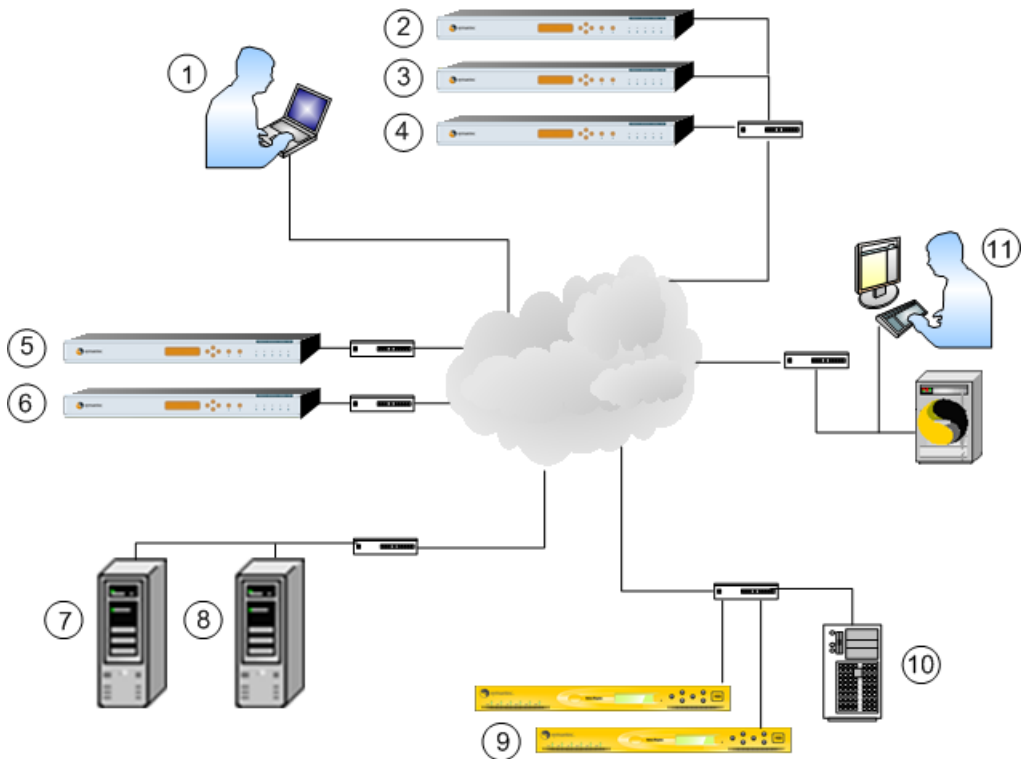


Table 3-2 describes the entities in Figure 3-2.

Table 3-2 Description of Figure 3-2

Callout	Installed component	Description
1	Security Gateway Management Interface (SGMI)	Used to manage Symantec security gateways locally
2	Symantec Gateway Security 5461 appliance v2.0	Corporate payroll office
3	Symantec Gateway Security 5461 appliance v2.0	Corporate payroll office
4	Symantec Gateway Security 5461 appliance v2.0	Corporate payroll office
5	Symantec Gateway Security 5440 appliance v2.0	Satellite sales office
6	Symantec Gateway Security 5440 appliance v2.0	Satellite sales office
7	Symantec Enterprise Firewall 8.0	Corporate headquarters
8	Symantec Enterprise Firewall 8.0	Corporate headquarters
9	Symantec Gateway Security appliances v1.0	Legacy security gateways sending events to SESA.
10	Remote log server	Forwards legacy security events to SESA.
11	SESA Console	Manages configurations and events for multiple security gateways.

When you have multiple security gateways with the same function, you can group them to make it easier to manage configurations.

Figure 3-2 shows three groups of security gateways. Each group uses a unique security policy that is designed to meet its needs and location settings that reflect its location and network configuration, as shown in Table 3-3:

Table 3-3 Security gateways with unique security policies

Callout	Function	Security policy	Location settings
2	Payroll office	Payroll	New York1
3	Reimbursement	Expenses	New York2
4	Equipment purchase	Purchasing	New York3

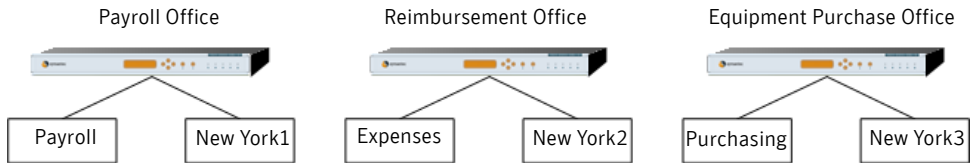
Table 3-3 Security gateways with unique security policies

Callout	Function	Security policy	Location settings
5	Satellite sales office	Sales_UK	London
6	Satellite sales office	Sales_FR	Paris
7	Corporate headquarters	Corporate1	HQ_Bldg1
8	Corporate headquarters	Corporate2	HQ_Bldg2

The following figures illustrate how you can simplify management by using a common security policy with multiple security gateways.

[Figure 3-3](#) shows the policy and location settings for the security gateways in New York.

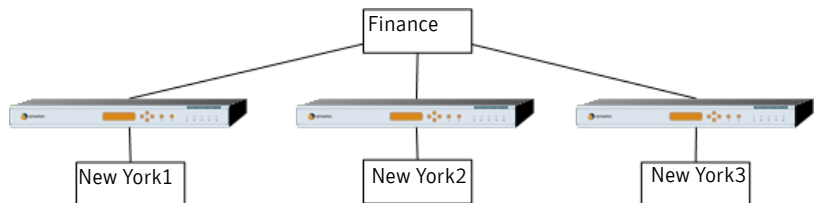
Figure 3-3 Initial security policies



To simplify the task of maintaining changes to multiple configurations, the security administrator reviewed the security policies for these security gateways and found that they could be combined into one policy.

As shown in [Figure 3-4](#), by assigning the new policy (Finance) to the three security gateways, the administrator can make configuration changes to one policy instead of the policies of each individual security gateway.

Figure 3-4 Combined security policies



Understanding how shared configurations are validated

Every security gateway is configured with a policy and location settings pair, which are considered to be associated.

In Symantec Advanced Manager, policy-location settings associations are designed using a one-to-many model, in which a policy may be associated with many locations, but a location can be associated with no more than one policy.

To understand how this model works, you must understand the chaining effect between configurations during validation and activation.

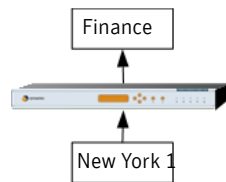
Configuration chaining

Configuration chaining describes the way configurations are validated.

In the example in [Figure 3-4](#), security gateways in the payroll, reimbursement, and equipment purchase offices all share the same global policy (Finance), but each has their own specific location settings (New York1, New York2, and New York3).

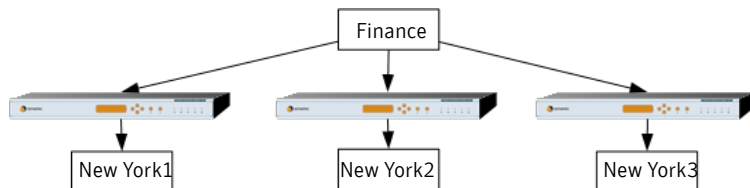
An administrator may need to modify only the New York1 location settings because of changes to that network. When the modified location settings are associated with the security gateway, Symantec Advanced Manager validates only with the security gateway for that office.

Figure 3-5 One-to-one location setting to policy validation



However, if the administrator changes the Finance policy and activates it, Symantec Advanced Manager validates the modified policy with the location settings for every security gateway that uses the Finance policy.

Figure 3-6 One-to-many policy to location setting validation



One-to-many policy relationship

The examples in “[Configuration chaining](#)” on page 36 show how Symantec Advanced Manager supports one-to many policy-location associations.

In a one-to-many environment, the effects of chained configurations are limited by associating policies and locations as follows:

- A single policy can have multiple location settings to which it is paired. For example, two security gateways can share the same sales policy, but have unique location settings because they reside in different offices.
- Location settings are bound to a single policy, regardless of the security gateway they are associated with. For example, two security gateways at the same office might have the same location settings, but that would imply that they also must have the same policy; the two security gateways cannot have two different policies under these circumstances.

Sharing policies without sharing locations

As shown in [Figure 3-4](#), your organization may have security gateways with different functional roles, but common goals in their defined security policies. Sharing the same policy among these security gateways simplifies management, and ensures that your organization’s security stance is consistent.

You should carefully consider sharing the same policy among multiple security gateways. Share policies when you have security gateways with the same security stance and identical functions, but in different geographic locations. For example, several regional offices that share the same security approach might share the same policy.

The benefits of a shared policy include the following:

- Eliminates duplication in configuration effort.
- Speeds up the process of making changes to multiple security gateways.
- Ensures that corporate security policy is adhered to across the company.

Requirements for using a shared policy include the following:

- Requires that the identical security policy is applicable at each location.
- Requires that references to logical labels in location settings are identical to ensure that each security gateway that is added can make use of rules.

Sharing both policies and location settings

You should only share both policies and location settings when you have identical functions in locations that are redundant, or locations where hardware High Availability/Load Balancing (HA/LB) is deployed but does not keep configurations identical between nodes. Additionally, sharing the same location settings can offer an overlay of WAN redundant locations that do not depend on virtual private networking.

Before you share both policies and location settings, you must create a superset of logical and topological information that includes the information for all the locations that you are defining.

Scalable management with organizational units

Scalable management introduces the concept of organizational units and physically separating security gateways in the SESA Console view. By separating security gateways in this manner, you can more clearly see how the entire network is structured. Organizational units also provide a mechanism to let member security gateways inherit an associated policy and location settings, simplifying management of many systems.

Organizational units

Organizational units are management objects that you can create using the SESA Console. They are used to store information about computers in the SESA Directory. Every security gateway that joins SESA is assigned to an organizational unit.

Although you can use the Default organizational unit for all your computers, by creating your own organizational units you can simplify the management of your security gateways. Like a company organization chart, your organizational units can logically group the machines you manage.

You can create your organizational units to represent departments within your organization, levels of access, geographical location, or any other logical grouping. If you prefer, you can assign every security gateway to the same organizational unit. However, you can gain greater benefit by planning and logically grouping systems into their own organizational units.

Every security gateway has an associated policy and location settings. Similarly, you can associate policy and location settings with an organizational unit, so that they can be inherited by any security gateway that is in the organizational unit. This mechanism lets you apply the same policy and location settings to multiple security gateways.

For security gateways in a cluster, you must associate configurations with the cluster's organizational unit. This enforces the requirement that all members of a cluster must share the same configuration. You cannot associate a policy or location settings to an individual cluster member. If you try to run the Associate Wizard on a clustered security gateway, you will receive an error message.

For instructions on creating an organizational unit, see the *Symantec Enterprise Security Architecture Administrator's Guide* or use the SESA Console Help system.

Moving a security gateway into an organizational unit

When a security gateway first joins SESA, the Join SESA Wizard requires that you select an organizational unit to which the security gateway will be assigned.

If you have not yet created organizational units, you must assign the security gateway to the Default organizational unit. Later, you can create organizational units to represent your security environment and move the security gateway into one of them.

If you create organizational units before you join security gateways to SESA, you can eliminate the step of having to move the security gateways to their intended destinations.

For more information, see the section on moving a computer to a different organizational unit in the *Symantec Enterprise Security Architecture Administrator's Guide*, or in the SESA Console Help.

Exporting and inheriting configurations

You place a security gateway in an organizational unit using the Join SESA Wizard.

Alternatively, if the organizational unit already has a policy and location settings associated with it, you can choose to inherit them. When you do this, changes that you make to the configuration do not have to be validated individually for each security gateway. You can edit either the policy or location settings associated with the organizational unit, and then validate and activate the changes once.

Inheriting both the policy and location settings from an organizational unit generally applies to either a clustered situation (because the cluster is represented as an organizational unit), or to a network of security gateways that are failovers for each other.

Understanding event management

This chapter includes the following topics:

- [Event management concepts](#)
- [Event management examples](#)
- [SESA event gating](#)
- [Viewing reports](#)

Event management concepts

Event management through SESA provides centralized event logging, alerting, and reporting. Event reports in SESA let you see security events and log messages in a tabular or graphical format.

Event management of security gateway log data is provided through Symantec Event Manager For Security Gateways.

Symantec Event Manager for Security Gateways is installed when you install Symantec Advanced Manager for Security Gateways.

If you only plan to use SESA to view and manage events, you can purchase and install Symantec Event Manager for Security Gateways separately.

For Symantec security gateways that are directly integrated with SESA, Symantec Event Manager for Security Gateways collects security information from each machine that has joined SESA and forwards it to the SESA Manager.

For legacy Symantec security gateway and third-party products, Symantec Event Manager for Firewall (included on the Symantec Advanced Manager for Security Gateways and Symantec Event Manager for Security Gateways CD-ROM) provides event management capabilities.

Through the use of a log server, Symantec Event Manager for Firewall forwards messages to the SESA Manager. These messages appear in the same reports as log messages that are forwarded by Symantec Event Manager for Security Gateways.

For third party log message, there are may be additional reports.

The benefits of event management through SESA are immediately apparent. Instead of having to go to each system, generate a usage report, and then manually cross check this report against reports from all other products, you can perform this task once, at one location, and collect reported events for all managed products.

Event management examples

Managing events through SESA offers a single point of access for all security gateways that send events to the SESA Manager.

The examples that are provided illustrate event management for a single security gateway and for multiple security gateways.

- When you manage events for a single security, you have the advantage of the firewall reports described in [“Security gateway reports”](#) on page 46.
- When you manage events for multiple security gateways, you have the added benefit that your reports display the event data from all of your security gateways.

The single biggest advantage of event management through SESA for a single security gateway is the organization of event data based on the reports you view. Once you have mastered viewing information for a single security gateway, managing events for multiple security gateway's events is minimal.

Single security gateway example

The single biggest advantage of event management through SESA for a single security gateway is the organization of event data in the Firewall reports you can view.

Figure 4-1 shows a single security gateway configured for event management.

Figure 4-1 Simple event management



Table 4-1 describes each of the entities in Figure 4-1.

Table 4-1 Descriptions of entities in Figure 4-1

Callout	Description
1	SESA Console.
2	SESA Manager.
3	Symantec Gateway Security 5420 appliances connected to SESA for event management only.

In this example, a single security gateway (3) sends events to SESA.

The events that are sent to SESA from this security gateway are determined by how you configure SESA event gating on the security gateway.

See “[SESA event gating](#)” on page 45.

Before viewing the reports, you should wait until the security gateway has had an opportunity to send some events to SESA.

Multiple security gateway example

When you configure event viewing of multiple security gateways, you are able to monitor the behavior of all these gateways from the single vantage point of the SESA Console.

This example shows event management for two sets of security gateways:

- Symantec Gateway Security 5400 series appliances
- Legacy Symantec security gateways on Symantec Security Gateway 100 appliances and a computer running Symantec Enterprise Firewall v7.0.

Figure 4-2 shows how SESA seamlessly handles event management of legacy and current security gateways. Reports appear similar to those seen in our first example, with the exception that now there are entries for each security gateway reporting to SESA.

Figure 4-2 Simple and legacy event management

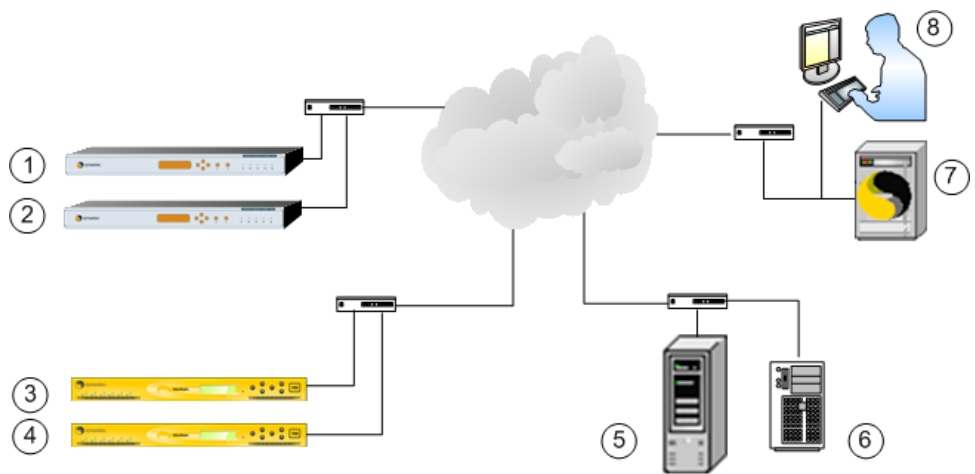


Table 4-2 gives a description of each of the entities found in Figure 4-2

Table 4-2 Descriptions of entities in Figure 4-2

Callout	Description
1	Symantec Gateway Security 5420 appliance v2.0 (joined for event management only).
2	Symantec Gateway Security 5420 appliance v2.0 (joined for event management only).
3	Symantec Gateway Security appliance v1.0 (joined for event management only).
4	Symantec Gateway Security appliance v1.0 (joined for event management only).
5	Symantec Enterprise Firewall with VPN version 7.0 joined for (event management only).
6	Symantec Event Manager for Firewall Log Server. The Symantec Event Collector for Security Gateways and SESA Agent are installed on this system. The Event Collector collects events from legacy systems, and the SESA Agent forwards them to the SESA Manager.

Table 4-2 Descriptions of entities in [Figure 4-2](#)

Callout	Description
7	SESA Manager.
8	SESA Console.

[Figure 4-2](#) shows the difference between the method used by legacy products to get events to SESA, and the method used by current security gateways.

- Legacy products use an intermediate log server to collect events.
The log server houses an agent that formats the messages, making them acceptable to SESA, and then forwards the events to the SESA Manager.
In [Figure 4-2](#), security gateways 3, 4, and 5 send their events to 6 (the log server). The log server then forwards those events to 1 (the SESA Manager).
- Current security gateways house the agent locally, and do not require an intermediate log server.
When a current security gateway joins SESA, the agent is downloaded to the security gateway and activated. The local agent performs the same functionality as the agent on the log server performs. It collects events from the local security gateway, formats them, and then forwards them to the SESA Manager.
In [Figure 4-2](#), events are collected on security gateways 1 and 2 and forwarded directly to 7 (the SESA Manager).

SESA event gating

Before you join a security gateway to SESA, you should configure SESA event gating. This feature of the local security gateway gives you some control over which messages are logged to SESA.

On the local security gateway, each log message that can be forwarded to SESA is assigned to a SESA event class or subclass. In addition, these messages belong to one of three categories:

- Always
These events are always forwarded to SESA and require no action.
- Configurable
Event classes that fall into the Sometimes category are listed on the Event Gating tab. You can select which classes of events you want to have sent to SESA.
When an event in a selected class occurs, a message is sent to the event collector.

- Never

These events cannot be forwarded to SESA

The majority of log messages that are sent to SESA are very similar to their counterparts in the local log file, but occasionally there are minor variations.

Note: By default, the security gateway logs only a small subset of events to SESA. Turning on all events incurs additional overhead, and may slow system performance. Carefully consider your selections when selecting the events to send to SESA.

Viewing reports

The event reports that are provided with Symantec Event Manager are displayed on the Event view tab of the SESA Console, in the Firewall Event Family and, for Symantec Gateway Security 5400 series appliances, in the Antivirus and Network Intrusion Event Families.

There are a wide variety of reports, designed to make it easy to identify important events. Some are very inclusive, showing all events in key categories. Others are more granular, such as a report of the most active Web users in the last 24 hours.

Some Firewall reports will only display data when you use SESA gating to enable the appropriate class or subclass. For example, if you have not enabled the statistics class, the Firewall connection statistics report will be empty.

For information, see the section on viewing reports in the *Symantec Advanced Manager for Security Gateways (Group 1) V2.0.1* and *Symantec Event Manager for Security Gateways (Group 1) V2.0.1 Administrator's Guide*.

Security gateway reports

The SESA Console displays events in event families. The Global reports are preconfigured reports provided with the SESA Manager. They typically use data gathered across all integrated security products that have been deployed in the environment that are sending events to SESA Managers.

When you install Symantec Advanced Manager for Security Gateways or Symantec Event Manager for Security Gateways on your SESA Manager, several sets of reports are installed:

- Firewall Event Family reports

The Firewall Event Family group of reports includes reports on all security gateways that report to SESA. This includes any Symantec Gateway

Security 5400 Series appliances or computer running Symantec Enterprise Firewall v8.0.

It also includes any legacy product, such as the Symantec Gateway Security 1.0 or VelociRaptor 1.5, and third-party security gateway products (separate purchase required).

- Security gateways (Group 1) reports
Similar to the Firewall Event Family reports, the Security gateways (Group 1) reports compile data received from Symantec security gateways that report to SESA.

The following two event families are created if your security gateway is a Symantec Gateway Security 5400 appliance. They are not supported for Symantec Enterprise Security v8.0:

- Anti Virus Event Family
The Anti Virus Event Family includes reports generated based on data received from any security gateway with a registered antivirus license. There are a handful of reports that are used exclusively by other Symantec products, and are not reported to by any security gateway product.
- Network Intrusion Event Family
The Network Intrusion Event Family includes reports generated based on data received from any security gateway with a registered intrusion detection license.

Two additional report families, Sensitive Content Filtering Event Family and Content Filtering Event Family, are also included when event management is enabled on the SESA Manager, but are not reported to by any security gateway.

Alerts and notifications

When you manage your firewall events through SESA, you can consolidate events by creating alerts.

These alerts can include:

- Alert filters that trigger alerts only when certain criteria are met.
For example, an alert configuration can be specific to a machine and a particular type of event for which you want to monitor.
- Alert notifications that are sent to specified users when an alert occurs.
You can specify that alert notifications are sent through paging, SNMP traps, email, and operating system event logs. You can also customized the notification message.
These alerts are in addition to notifications available on the security gateway.

Preparing to integrate security gateways with SESA

This chapter includes the following topics:

- [Planning for SESA integration](#)
- [Analyzing your security needs](#)
- [Required software](#)
- [Planning example](#)
- [Choosing your starting point](#)
- [Determining installation options and order](#)

Planning for SESA integration

Planning how you will use Symantec Advanced Manager to integrate your existing and planned security gateways with SESA is crucial to your success. In particular, by planning logical groupings of your security gateways, you can take full advantage of Symantec Advanced Manager's ability to deploy configurations and configuration updates to multiple gateways.

You may already have your security gateways in place, or you may be planning to add security gateways to protect your enterprise. In either case, getting a high level picture of your security gateway topology will help you decide how to manage your security gateway configurations using Symantec Advanced Manager.

Analyzing your security needs

To decide how to use Symantec Advanced Manager to manage your security gateways, you can ask yourself some simple questions. They are informal and representative rather than exhaustive.

As you review these questions, others may occur to you.

Table 5-1 Planning questions

Question	Examples
What do you want to protect?	■ Networks ■ Servers Mail Web (Internal / External) Departmental ■ Desktops ■ Users
How is your security environment organized?	■ By function ■ By location ■ By access rights
How do your security policies protect your resources?	■ What are your corporate policies? What traffic is allowed through? What traffic is blocked? ■ Can your security gateways share policies? ■ How often are policies modified? ■ Who does the configuration?
What security gateways protect your resources?	■ What Symantec security gateways? ■ What third party firewalls? ■ How do you group those gateways? ■ How do you modify policies on those gateways?
How will you deploy and configure SESA?	■ Inside the security perimeter? ■ Outside the security perimeter? ■ Only to manage security gateways? ■ To manage other security products?
How do you manage events	■ Who monitors your security gateways? ■ How do you view events for multiple gateways? ■ How do you use event data in reports?

As you evaluate your security posture, you can plan how to reflect it in SESA.

Required software

To use Symantec Advanced Manager for Security Gateways and Symantec Event Manager for Security Gateways, you must install and configure the SESA Foundation Pack and one or more security gateways.

SESA Foundation Pack

You must separately purchase, install, and configure the SESA Foundation Pack before you can install Symantec Advanced Manager and/or Symantec Event Manager.

For a description of the components of the SESA Foundation, see [“Understanding SESA management”](#) on page 19.

For deployment and installation instructions, see the *Symantec Enterprise Security Architecture Installation Guide*.

For configuration instructions, see the *Symantec Enterprise Security Architecture Administrator’s Guide*.

Security gateways

You must have installed one of more of the following security gateways:

- For Symantec Advanced Manager for Security Gateways:
 - Symantec Gateway Security 5400 appliances
For installation instructions, see the *Symantec Gateway Security 5400 Series Installation Guide*.
 - Symantec Enterprise Firewall, version 8.0
For installation instructions, see the *Symantec Enterprise Firewall Installation Guide*.
- For event collection and management by Symantec Event Manager for Security Gateways:
 - Symantec Gateway Security 5400 appliances
 - Symantec Enterprise Firewall, version 8.0
 - * Symantec Enterprise Firewall, version 7.0.x
 - * Symantec Gateway Security, version 1.0: models 5110, 5200, 5300, and 5310 (firewall events only)

Planning example

- * Symantec VelociRaptor, version 1.5: models 1100, 1200, 1300, and 1310

Also supports older VelociRaptor hardware models that have been upgraded to version 1.5 software.

- * Third-party products (requires separate purchase)
For installation instructions, see the documentation provided with these products.

* Security products that are marked with an asterisk do not have integrated SESA support. To view events for these products in SESA, you must also install the Symantec Event Manager for Firewall that is included on your product CD-ROM. For installation instructions, see [“Installing Symantec Event Manager for Firewall”](#) on page 119.

Planning example

[Figure 5-1](#) shows a high level plan to manage security gateway configurations using Symantec Advanced Manager.

It represents an organization with the following characteristics:

- The organization is geographically dispersed, with networks in several locations.
- Security gateways are deployed according to geography.
- Multiple Symantec Gateway Security 5420 appliances are clustered for High Availability /Load Balancing (1). These protect all departments in one location.
- A combination of Symantec Gateway Security 5400 series appliances and computers with Symantec Enterprise Firewall v8.0 protect all departments in a second location (3).

- Security gateways are deployed in a third location, from which the company simply wants to collect and manage event data (4).
- Legacy Symantec security gateways are deployed at a fourth location, from which the company wants to collect and manage event data (6).

Figure 5-1 Example security configuration

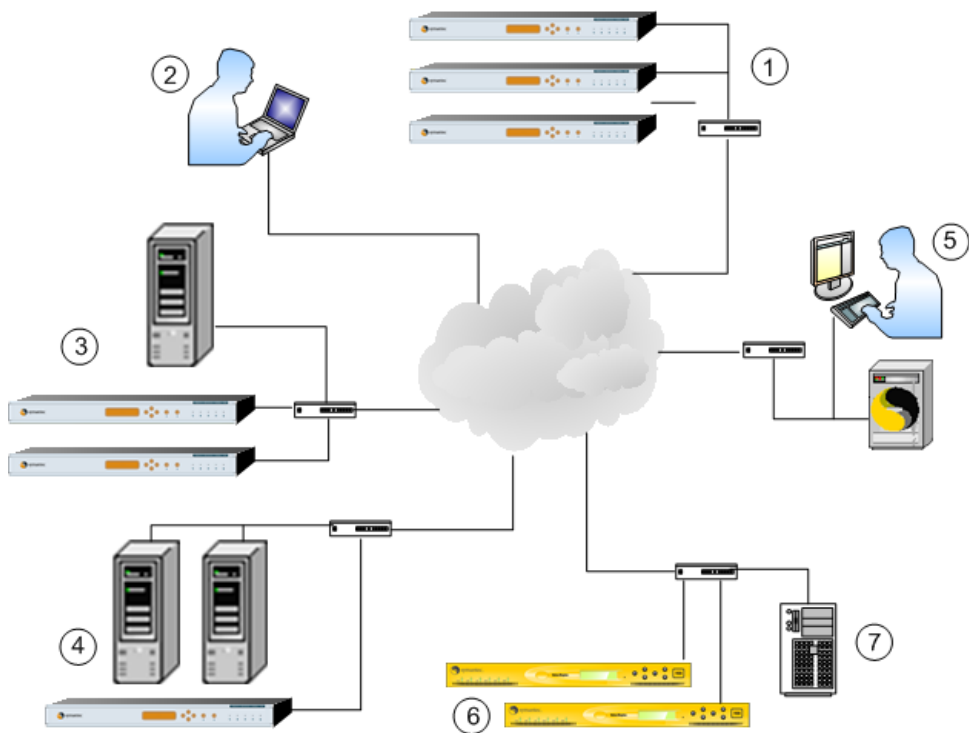


Table 5-2 describes the components of this configuration:

Table 5-2 Description of Figure 5-1

Callout	Installed component	Management description
1	Cluster of Symantec Gateway Security 5420 appliances v2.0	When you join one cluster member to SESA, all of the security gateways in this cluster are automatically placed in the organizational unit that you specify, enabling you to manage the cluster using Symantec Advanced Manager.
2	Security Gateway Management Interface (SGMI)	When you need to make changes to local settings, you use the SGMI to manage your Symantec security gateways.

Table 5-2 Description of [Figure 5-1](#) (Continued)

Callout	Installed component	Management description
3	Symantec Enterprise Firewall v8.0 Symantec Gateway Security 5440 appliance v2.0 Symantec Gateway Security 5460 appliance v2.0	You join these security gateways to SESA for management using Symantec Advanced Manager. You can place them in an organizational units that you have already created in SESA, or in the Default or Managers organizational unit.
4	Symantec Enterprise Firewall 8.0 Symantec Enterprise Firewall 8.0 Symantec Gateway Security 5440 appliance v2.0	You join these security gateways to SESA only for event management by the Symantec Event Manager that is installed when you install Symantec Advanced Manager. SESA automatically places these security gateways in the Default organizational unit.
5	SESA Console	You use the SESA Console to manage your security gateways using Symantec Advanced Manager and to view and manage events using Symantec Event Manager.
6	Symantec Gateway Security appliances v1.0	You use Symantec Event Manager to collect events from legacy gateways and send them to SESA. There is no configuration management.
7	Remote log server	You install the event collection components of Symantec Event Manager for Firewall on the remote log server to forward events to SESA.

Choosing your starting point

As you plan for management through SESA, you must decide how you will create your initial security gateway configuration, and how you will share configurations among security gateways.

There are a number of possible scenarios. All require you to complete the following basic configuration on the local security gateway by using the Security Gateway Management Interface (SGMI):

- Run the System Setup Wizard to make sure that your network interfaces, licenses, and other system settings are set correctly.
- In the Monitoring window, use the SESA event gating tab to select which events are forwarded to SESA.
- Back up your configuration.

After the local prerequisites are met, each option involves additional choices about where policy and location settings are initially configured, the method of joining SESA, and how Symantec Advanced Management is used to update and activate policy and location settings:

Table 5-3 Initial configuration options for advanced management

Initial configuration	Method for joining SESA	Advanced management
Use an existing security gateway configuration. (Recommended)		
Verify the current policy and location settings locally.	Export the configuration of the local security gateway to SESA.	Modify the configurations in SESA and activate them on connected computers.
Create the initial configuration locally. (Recommended)		
Create and verify the policy and location settings locally.	Export the configuration of the local security gateway to SESA.	Modify the configurations in SESA and activate them on connected computers.
Create the initial configuration in SESA.		
Use Symantec Advanced Manager to configure policy and location settings.	Assign each security gateway to an organizational unit that has been created for it in SESA.	Use Symantec Advanced Manager to create policies and location settings. When new security gateways join SESA, associate the policies and location settings with them.
Use an existing security gateway configuration from a member of a cluster.		
Verify the policy and location settings locally on one member of the cluster.	Join the cluster member to SESA. Name the organizational unit to which it is added and name the policy and location settings.	Modify the cluster policy and location settings in SESA. Activate changes on cluster members by way of their organizational unit.
Use an existing security gateway configuration associated with an organizational unit.		
Validate the policy and location settings in SESA.	Join the security gateway to SESA. Select the organizational unit and inherit its policy and location settings	Modify the organizational unit's configuration in SESA. Activate changes by way of the organizational unit.

Determining installation options and order

The components you install and the order in which you install them depend on the software you have purchased, the security gateways that you are currently managing, and additional security gateways that you want to manage.

This section provides a roadmap to help you identify the software components that you need to install and the sections of this guide that document the installation processes.

Note: In the following sections, when Symantec Event Manager for Security Gateways is required, you can also install Symantec Advanced Manager for Security Gateways. Symantec Advanced Manager for Security Gateways includes Symantec Event Manager for Security Gateways.

New installations

The simplest scenarios apply when you are not currently managing any security gateways through SESA:

- To manage Symantec Security Gateway 5400 Series appliances and Symantec Enterprise Firewall v8.0, on the SESA Manager, install one of the following:
 - To manage both configurations and events, install Symantec Advanced Manager for Security Gateways (Group 1) v2.0.1.
See [“Installing Symantec Advanced Manager for Security Gateways”](#) on page 64.
 - To manage events only, install Symantec Event Manager for Security Gateways (Group 1) v2.0.1.
See [“Installing Symantec Event Manager for Security Gateways”](#) on page 76.
- To manage events from legacy Symantec security gateways, do the following:
 - On the SESA Manager, install Symantec Event Manager for Security Gateways (Group 1) v2.0.1.
See [“Installing Symantec Event Manager for Security Gateways”](#) on page 76.
 - On a Microsoft Windows or Sun Solaris 8 or 9 system, install and configure the Remote Log utility.
See [“Installing the Remote Log utility on the log server”](#) on page 116.

- On the remote log server, install the Symantec Event Manager for Firewall components.
 See [“Installing Symantec Event Manager for Firewall components on the log server”](#) on page 127.
- To manage events from third-party security gateways, you must separately purchase a Symantec event collector for the security gateway.
 Do the following:
 - On the SESA Manager, install Symantec Event Manager for Security Gateways (Group 1) v2.0.1.
 See [“Installing Symantec Event Manager for Security Gateways”](#) on page 76.
 - On the third-party security gateway, install the Symantec Event Manager for Firewall (found on the Symantec Event Manager for Security Gateways CD-ROM) and the separately purchased third-party event collector.
 Follow the instructions in the documentation for the third-party event collector.
- To manage a combination of v8.0 Symantec security gateway configurations and events, events from legacy Symantec security gateways, and events from third-party security gateways, combine the installation instructions described in this section.

Upgrading from Symantec Advanced Manager for Security Gateways v2.0 and Symantec Event Manager for Security Gateways v2.0

You can easily upgrade if you are already managing security gateway configurations and events in SESA with Symantec Advanced Manager for Security Gateways v2.0 or Symantec Event Manager for Security Gateways v2.0.

For any of the management scenarios described in [“New installations”](#) on page 56, complete the appropriate upgrade procedure when you install the v2.0.1 products.

For example, to upgrade for event management only, see [“Upgrading from Symantec Event Manager for Security Gateways v2.0 to Symantec Event Manager for Security Gateways v2.0.1”](#) on page 80.

After you upgrade, you can also add additional types of security gateway management to your configuration. Depending on the software you have purchased, you can follow any of the management scenarios described in [“New installations”](#) on page 56.

Upgrading from Symantec Event Manager for Firewall v1.0

If you are currently using Symantec Event Manager for Firewall v1.0 to collect events from legacy Symantec security gateways and third-party security gateways, you can upgrade to Symantec Advanced Manager for Security Gateways v2.0.1 or Symantec Event Manager for Security Gateways v2.0.1.

This upgrade requires you to uninstall Symantec Event Manager for Firewall v1.0 and then install either Symantec Advanced Manager for Security Gateways v2.0.1 or Symantec Event Manager for Security Gateways v2.0.1.

See [“Upgrading from Symantec Event Manager for Firewall v1.0 to Symantec Event Manager for Security Gateways v2.0.1”](#) on page 134.

After you upgrade, you can also add additional types of security gateway management to your configuration. Depending on the software you have purchased, you can follow any of the management scenarios described in [“New installations”](#) on page 56.

Integrating Symantec security gateways with SESA

This section includes the following topics:

- [Installing Symantec Advanced Manager for Security Gateways](#)
- [Installing Symantec Event Manager for Security Gateways](#)
- [Joining security gateways to SESA](#)

Installing Symantec Advanced Manager for Security Gateways

This chapter includes the following topics:

- [Symantec Advanced Manager for Security Gateways \(Group 1\) v 2.0.1 installation CD-ROM contents](#)
- [Installing Symantec Advanced Manager for Security Gateways](#)
- [Verifying the Symantec Advanced Manager installation](#)
- [Upgrading from Symantec Advanced Manager for Security Gateways v2.0 to Symantec Advanced Manager for Security Gateways v2.0.1](#)
- [Upgrading from Symantec Event Manager for Security Gateways v2.0 to Symantec Advanced Manager for Security Gateways V2.0.1](#)
- [Tuning Apache Tomcat memory usage on the SESA Manager](#)
- [Uninstalling Symantec Advanced Manager](#)

About installing Symantec Advanced Manager

Symantec Advanced Manager for Security Gateways provides advanced management capabilities for your security gateways.

Symantec Advanced Manager for Security Gateways lets you centrally manage and distribute your security gateway configurations to multiple security gateways.

When you install Symantec Advanced Manager, you also install Symantec Event Manager for Security Gateways, which provides centralized logging, alerting, and reports based on your security gateway event logs.

Symantec Advanced Manager for Security Gateways (Group 1) v 2.0.1 installation CD-ROM contents

The installation media for Symantec Advanced Manager for Security Gateways includes Symantec Event Manager for Security Gateways and Symantec Event Manager for Firewall.

Table 6-1 Symantec Advanced Manager for Security Gateways (Group 1) v 2.0.1 CD-ROM contents

CD folder	Contents
Adobe\Windows\AdbeRdr60_enu_full.exe	Version 6.0 of the Adobe Acrobat reader.
EM_Firewall_1_0\	Symantec Event Manager for Firewall files.
EM_Firewall_1_0\Solaris	■ install ■ SEFCollector.tar
EM_Firewall_1_0\Solaris\AgtInst	Files to install the SESA Agent in a Solaris 8 environment.
EM_Firewall_1_0\Solaris\AgtInst\SOLARIS8	■ adentd ■ libjsunutil.so
EM_Firewall_1_0\techpubs	■ ESD.GlobalEULA.Standard.txt ■ SEM_Firewall_Intg.pdf <i>Symantec Event Manager for Firewall Integration Guide</i> ■ SEM_Firewall_RN.pdf <i>Symantec Event Manager for Firewall Release Notes</i>
EM_Firewall_1_0\Windows	■ Data1.cab ■ isscript.msi ■ JREGENT.DLL ■ JWINUTIL.DLL ■ launcher.settings ■ libjsunutil.so ■ setup.exe ■ setup.jar ■ Symantec Event Manager for Firewall.msi

Table 6-1 Symantec Advanced Manager for Security Gateways (Group 1)
v 2.0.1 CD-ROM contents (Continued)

CD folder	Contents
EM_Firewall_1_0\Windows\Agtinst	Files to install the SESA Agent.
SESA\	Symantec Advanced Manager and Symantec Event Manager for Security Gateways files.
SESA\Documentation	■ AdvEventMngr_Admin.pdf <i>Symantec Advanced Manager for Security Gateways (Group1) and Symantec Event Manager for Security Gateways (Group1) Administrator's Guide</i> ■ AdvEventMngr_Integrate.pdf <i>Symantec Advanced Manager for Security Gateways (Group1) and Symantec Event Manager for Security Gateways (Group1) Integration Guide</i> ■ AdvEventMngr_ReleaseNotes.pdf <i>Symantec Advanced Manager for Security Gateways (Group1) and Symantec Event Manager for Security Gateways (Group1) Release Notes</i>
SESA\SIPI	Installation files for Symantec Advanced Manager and Symantec Event Manager for Security Gateways.

Before you install

Before you install Symantec Advanced Manager for Security Gateways, do the following:

- Verify that the SESA Manager is running on the system on which you will install.
- In the SESA Console, on the Configurations tab, determine whether Symantec Event Manager for Firewall is installed for event management of legacy and third-party security gateways.
 - If Symantec Event Manager for Firewall is not installed, proceed with the installation of Symantec Advanced Manager for Firewall.
 - If Symantec Event Manager for Firewall is installed, follow the instructions in [“Upgrading from Symantec Event Manager for Firewall v1.0 to Symantec Event Manager for Security Gateways v2.0.1”](#) on page 134.

- Obtain the following information from your SESA administrator:
 - SESA Domain Administrator Name
 - SESA Domain Administrator Password
 - Host Name or IP Address of the SESA Directory
 - Secure Directory Port

Installing Symantec Advanced Manager for Security Gateways

The Symantec Advanced Manager for Security Gateways includes both policy configuration and event logging, alerting, and reporting. If you install the Symantec Advanced Manager, you do not need to install the Symantec Event Manager for Security Gateways; it is installed automatically as part of this installation. You install Symantec Advanced Manager on the SESA Manager.

After you install the software on the SESA Manager and join your first security gateway to SESA, all subsequent security gateways can join SESA without any additional installation requirement on the SESA Manager.

To install Symantec Advanced Manager

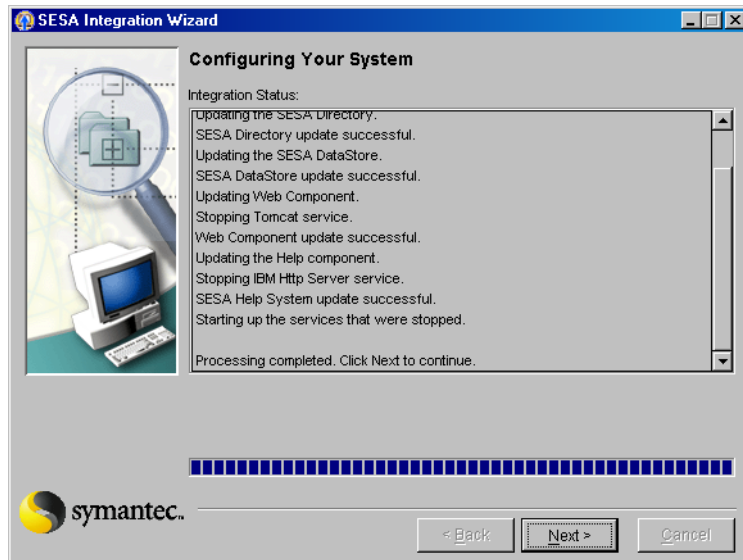
- 1 On the SESA Manager, insert the *Symantec Advanced Manager for Security Gateways (Group 1) v 2.0.1* installation CD-ROM into the CD-ROM drive.
- 2 Browse to SESA/SIPI/, and then double-click **Install.bat**.
A command window displays, showing the preparation for the installation, followed by a License and Warranty Agreement.
- 3 In the License and Warranty Agreement dialog box, read the license agreement, and then do one of the following:
 - If you accept the license agreement, click **Accept**.
 - If you do not accept the license agreement, click **Don't Accept**.
If you do not accept the license agreement, you cannot continue with the installation procedure.
- 4 On the Welcome to SESA Integration Wizard panel, click **Next**.

- 5 In the SESA Integration Requirements panel, click **Next**.

- 6 In the SESA Domain Administrator Information panel, do the following:

- | | |
|---|--|
| SESA Domain Administrator Name | Type the domain administrator's user name. |
| SESA Domain Administrator Password | Type the domain administrator's password. |
| Host Name or IP Address of SESA Directory | <p>Type one of the following:</p> <ul style="list-style-type: none"> ■ If SESA is using default, anonymous SSL communications, the IP address of the computer on which the SESA Directory is installed (it may be the same as the SESA Manager IP address if they are both installed on the same computer). You can also type localhost. ■ If SESA is using authenticated SSL communication, the host name of the SESA Directory computer. For example, mycomputer.com. <p>For more information on the SESA default, anonymous SSL, and upgrading to authenticated SSL, see the <i>Symantec Enterprise Security Architecture Installation Guide</i>.</p> |
| Secure Directory Port | <p>Type the port number.</p> <p>The typical directory port number is 636.</p> |

- 7 Click **Next**.
- 8 In the Ready to proceed panel, do one of the following:
 - To change your settings, click **Back**.
 - To proceed, click **Next**.



In the Configuring Your System panel, the Integration Status window shows the progress of the installation.

This process may take several minutes.

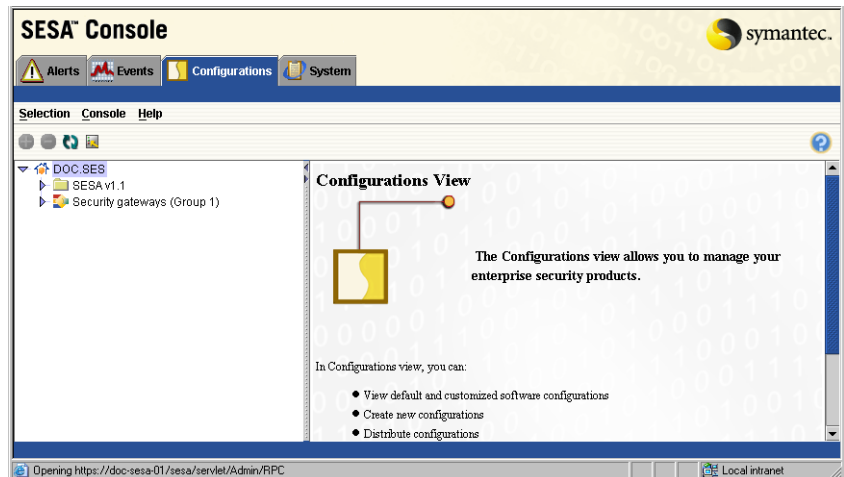
- 9 When the Processing completed message appears at the bottom of the window, click **Next**.
- 10 In the SESA Integration Successful panel, click **Finish**.

Verifying the Symantec Advanced Manager installation

To verify the installation, log on to the SESA Console. In the Configurations view tab, confirm that Security Gateways (Group 1) is listed.

To verify the Symantec Advanced Manager installation

- 1 To display the SESA Console, do one of the following:
 - If you are working on the SESA Manager computer, on the Windows taskbar, click **Start > Programs > Symantec Enterprise Security > SESA Console**.
 - If you are not working directly on the SESA Manager computer, in a browser window type the URL of the SESA Manager.
- 2 Log on to the SESA Console using the Domain Administrator account.
- 3 In the SESA Console, on the Configuration view tab, in the left pane, confirm that Security Gateways (Group 1) is one of the listed products.



Upgrading from Symantec Advanced Manager for Security Gateways v2.0 to Symantec Advanced Manager for Security Gateways v2.0.1

If you are already running Symantec Advanced Manager for Security Gateways (Group 1) v2.0 to manage Symantec security gateway appliances, you can upgrade to Symantec Advanced Manager for Security Gateways (Group 1) v2.0.1 without uninstalling.

To upgrade from Symantec Advanced Manager for Security Gateways v2.0

- 1 Back up your SESA Directory.
See the section on archiving a SESA Directory in the *Symantec Enterprise Security Architecture Installation Guide*.
- 2 Back up your SESA DataStore.
See the following Symantec Knowledge Base article for back up instructions:
<http://service1.symantec.com/SUPPORT/ent-gate.nsf/docid/2003042816055954>
This article, “How to migrate a SESA DB2 DataStore to a different computer”, describes the back up and restore process.
- 3 Perform the installation procedure that is described in “[Installing Symantec Advanced Manager for Security Gateways](#)” on page 64.

Upgrading from Symantec Event Manager for Security Gateways v2.0 to Symantec Advanced Manager for Security Gateways V2.0.1

If you are running Symantec Event Manager for Security Gateways (Group 1) v2.0 to view events from Symantec security gateway appliances, you can upgrade to Symantec Advanced Manager for Security Gateways (Group 1) v2.0.1. This upgrade gives you the added ability to manage your security gateway configurations through the SESA Console.

To upgrade from Symantec Event Manager for Security Gateways v2.0

- 1 Back up your SESA Directory.
See the section on archiving a SESA Directory in the *Symantec Enterprise Security Architecture Installation Guide*.

- 2 Back up your SESA DataStore.
See the following Symantec Knowledge Base article for back up instructions:
<http://service1.symantec.com/SUPPORT/ent-gate.nsf/docid/2003042816055954>
This article, “How to migrate a SESA DB2 DataStore to a different computer”, describes the back up and restore process.
- 3 Perform the installation procedure that is described in “[Installing Symantec Advanced Manager for Security Gateways](#)” on page 64.

Tuning Apache Tomcat memory usage on the SESA Manager

The Apache Tomcat service is installed on the SESA Manager as part of the SESA installation. It is used to for SESA Manager processing.

Before you begin managing security gateways using SESA, you can increase the amount of minimum and maximum memory that is used by the Apache Tomcat service, especially if you have installed multiple security products on SESA.

Your Symantec Advanced Manager for Security Gateways (Group 1) CD-ROM includes a setTomcatMemSize tool that allows you to change the minimum and maximum memory.

Increasing the memory used by the Apache Tomcat service

You can use setTomcatMemSize tool to increase memory available to the Apache Tomcat service if one of the following conditions are true:

- Apache Tomcat is using the default values.
- The new values you supply are greater than the current settings.

To increase the memory used by Apache Tomcat

- 1 On the SESA Manager, determine the amount of RAM.
- 2 Insert the *Symantec Advanced Manager for Security Gateways (Group 1) v 2.0.1* installation CD-ROM into the CD-ROM drive.
- 3 Open a DOS window.
- 4 Change to the following location:
`<DRIVE>:\SESA\SIPT\`
where <DRIVE> is the drive in which you inserted the CD-ROM.

- 5 To determine the minimum and maximum memory values that are currently being used by the Apache Tomcat service, type the following command:

```
setTomcatMemSize -r
```

The default values are:

MIN 128 MB

MAX 512 MB

- 6 To increase the minimum and maximum memory used by the Apache Tomcat service, enter a command in the following format:

```
setTomcatMemSize <MIN> <MAX>
```

where <MIN> is the minimum memory size in MBs and <MAX> is the maximum memory size in MBs. If you supply only one parameter, both the minimum and maximum memory used by Tomcat is set to that value. You should set the minimum value to at least 256 MB. The values cannot exceed the amount of available RAM.
- 7 Press **Enter**.
The Apache Tomcat service is automatically restarted using the modified values.
- 8 Close the DOS window.

Lowering the memory usage values

When you increase the memory values, changes are made to the registry.

If you change both the minimum and maximum memory values, two new string value entries are added in the following registry location:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Apache Tomcat\Parameters\JVM Option Number <N>

where <N> is the next consecutively available JVM number.

The string values have the following formats, based on the values you specified when you executed the setTomcatMemSize command:

-Xms<NNN> Where <NNN> is the minimum memory value

-Xmx<NNN> Where <NNN> is the maximum memory value

If you find that increasing the memory usage values causes poor performance, you can lower the values.

Caution: You should not attempt to modify the registry unless you are familiar with using the regedit editor.

To lower the memory usage values

- 1 On the SESA Manager, in the Run window, type **regedit**.
- 2 In the left pane, Navigate to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Apache Tomcat\Parameters.
- 3 In the right pane, locate the last two JVM Option Number entries.
- 4 Delete the string values.
- 5 Rerun the setTomcatMemSize tool to set new values.
The new values do not take effect until the Apache Tomcat server is restarted.

Uninstalling Symantec Advanced Manager

Before uninstalling, ensure that the SESA Manager is running on this system. SESA Manager must be operating properly prior to uninstalling any SESA components.

Also, before you begin, obtain the following information from your SESA administrator:

- SESA Domain Administrator Name
- SESA Domain Administrator Password
- Host Name or IP Address of the SESA Directory
- Secure Directory Port

To uninstall the Symantec Advanced Manager for Security Gateways

- 1 Insert the *Symantec Advanced Manager for Security Gateways (Group 1) v 2.0.1* CD-ROM into the CD-ROM drive on the SESA Manager computer.
- 2 Browse to SESA/SIPI/, and then double-click **Uninstall.bat**.
A command window shows the preparations for the uninstall procedure.
- 3 On the Welcome to SESA Integration Wizard panel, click **Next**.
- 4 In the SESA Integration Requirements panel, click **Next**.

5 In the SESA Domain Administrator Information panel, do the following:

SESA Domain Administrator Name	Type the domain administrator's user name.
SESA Domain Administrator Password	Type the domain administrator's password.
Host Name or IP Address of SESA Directory	Type one of the following: ■ If SESA is using default, anonymous SSL communications, the IP address of the computer on which the SESA Directory is installed (it may be the same as the SESA Manager IP address if they are both installed on the same computer). You can also type localhost. ■ If SESA is using authenticated SSL communication, the host name of the SESA Directory computer. For example, mycomputer.com. For more information on the SESA default, anonymous SSL, and upgrading to authenticated SSL, see the <i>Symantec Enterprise Security Architecture Installation Guide</i>.
Secure Directory Port	Type the port number. The typical directory port number is 636.

6 Click **Next**.

7 In the Ready to proceed panel, do one of the following:

- To change your settings, click **Back**.
- To proceed, click **Next**.

In the Configuring Your System panel, the Integration Status window shows the progress of the removal of Symantec Advanced Manager. This process may take several minutes.

8 When the Processing completed message appears at the bottom of the window, click **Next**.

9 In the SESA Integration Successful panel, click **Finish**.

Installing Symantec Event Manager for Security Gateways

This chapter includes the following topics:

- [Symantec Event Manager for Security Gateways \(Group 1\) v 2.0.1 installation CD-ROM contents](#)
- [Before you install](#)
- [Installing Symantec Event Manager for Security Gateways](#)
- [Verifying the Symantec Event Manager installation](#)
- [Upgrading from Symantec Event Manager for Security Gateways v2.0 to Symantec Event Manager for Security Gateways v2.0.1](#)
- [Uninstalling Symantec Event Manager](#)

About installing Symantec Event Manager

If you installed the Symantec Advanced Manager for Security Gateways, you do not need to install the Symantec Event Manager for Security Gateways; event management is included with the Symantec Advanced Manager.

You can use Symantec Event Manager for centralized logging, alerting, and reporting across Symantec's security gateway protection solutions and select third-party firewall products. See [“Event management concepts”](#) on page 41.

You can install the Symantec Event Manager when you want only logging, alerting, and reporting for the security gateways. After installing the software on the SESA Manager and joining your first security gateway to SESA, all

subsequent security gateways can join SESA without any additional installation requirement on the SESA Manager.

Symantec Event Manager for Security Gateways (Group 1) v 2.0.1 installation CD-ROM contents

The installation media for Symantec Event Manager for Security Gateways includes Symantec Event Manager for Firewall.

Table 7-1 Symantec Event Manager for Security Gateways (Group 1) v 2.0.1 installation CD-ROM contents

CD folder	Contents
Adobe\Windows\AdbRdr60_enu_full.exe	Version 6.0 of the Adobe Acrobat reader.
EM_Firewall_1_0\	Symantec Event Manager for Firewall files.
EM_Firewall_1_0\Solaris	■ install ■ SEFCollector.tar
EM_Firewall_1_0\Solaris\AgtInst	Files to install the SESA Agent in a Solaris 8 environment.
EM_Firewall_1_0\Solaris\AgtInst\SOLARIS8	■ adentd ■ libjsunutil.so
EM_Firewall_1_0\techpubs	■ ESD.GlobalEULA.Standard.txt ■ SEM_Firewall_Intg.pdf <i>Symantec Event Manager for Firewall Integration Guide</i> ■ SEM_Firewall_RN.pdf <i>Symantec Event Manager for Firewall Release Notes</i>
EM_Firewall_1_0\Windows	■ Data1.cab ■ isscript.msi ■ JREGENT.DLL ■ JWINUTIL.DLL ■ launcher.settings ■ libjsunutil.so ■ setup.exe ■ setup.jar ■ Symantec Event Manager for Firewall.msi
EM_Firewall_1_0\Windows\Agtinst	Files to install the SESA Agent.

Table 7-1 Symantec Event Manager for Security Gateways (Group 1) v 2.0.1 installation CD-ROM contents (Continued)

CD folder	Contents
SESA\	Symantec Event Manager for Security Gateways files.
SESA\Documentation	■ AdvEventMngr_Admin.pdf <i>Symantec Advanced Manager for Security Gateways (Group1) and Symantec Event Manager for Security Gateways (Group1) Administrator's Guide</i> ■ AdvEventMngr_Integrate.pdf <i>Symantec Advanced Manager for Security Gateways (Group1) and Symantec Event Manager for Security Gateways (Group1) Integration Guide</i> ■ AdvEventMngr_ReleaseNotes.pdf <i>Symantec Advanced Manager for Security Gateways (Group1) and Symantec Event Manager for Security Gateways (Group1) Release Notes</i>
SESA\SIPI	Installation files for Symantec Event Manager for Security Gateways.

Before you install

Before you install Symantec Event Manager for Security Gateways, do the following:

- Verify that the SESA Manager is running on the system on which you will install.
- In the SESA Console, on the Configurations tab, determine whether Symantec Event Manager for Firewall is installed for event management of legacy and third-party security gateways.
 - If Symantec Event Manager for Firewall is not installed, proceed with the installation of Symantec Event Manager for Security Gateways.
 - If Symantec Event Manager for Firewall is installed, follow the instructions in [“Upgrading from Symantec Event Manager for Firewall v1.0 to Symantec Event Manager for Security Gateways v2.0.1”](#) on page 134.

- Obtain the following information from your SESA administrator:
 - SESA Domain Administrator Name
 - SESA Domain Administrator Password
 - Host Name or IP Address of the SESA Directory
 - Secure Directory Port

Installing Symantec Event Manager for Security Gateways

You install Symantec Event Manager for Security Gateways on the SESA Manager computer.

To install Symantec Event Manager for Security Gateways

- 1 Insert the *Symantec Event Manager for Security Gateways (Group 1) v 2.0.1* installation CD-ROM into the CD-ROM drive on the SESA Manager computer.
- 2 Browse to SESA/SIPI/, and then double-click **install.bat**.
A command window displays, showing the preparation for the installation, followed by a License and Warranty Agreement.
- 3 In the License and Warranty Agreement dialog box, read the license agreement, and then do one of the following:
 - If you accept the license agreement, click **Accept**.
 - If you do not accept the license agreement, click **Don't Accept**.
If you do not accept the license agreement, you cannot continue with the installation procedure.
- 4 In the Welcome to SESA Integration Wizard panel, click **Next**.

- 5 In the SESA Integration Requirements panel, verify that the SESA Manager is running on the system, and then click **Next**.

- 6 In the SESA Domain Administrator Information panel, do the following:

- | | |
|---|---|
| SESA Domain Administrator Name | Type the domain administrator's user name. |
| SESA Domain Administrator Password | Type the domain administrator's password. |
| Host Name or IP Address of SESA Directory | <p>Type one of the following:</p> <ul style="list-style-type: none"> ■ If SESA is using default, anonymous SSL communications, the IP address of the computer on which the SESA Directory is installed (it may be the same as the SESA Manager IP address if they are both installed on the same computer). You can also type localhost. ■ If SESA is using authenticated SSL communication, the host name of the SESA Directory computer. For example, mycomputer.com. |

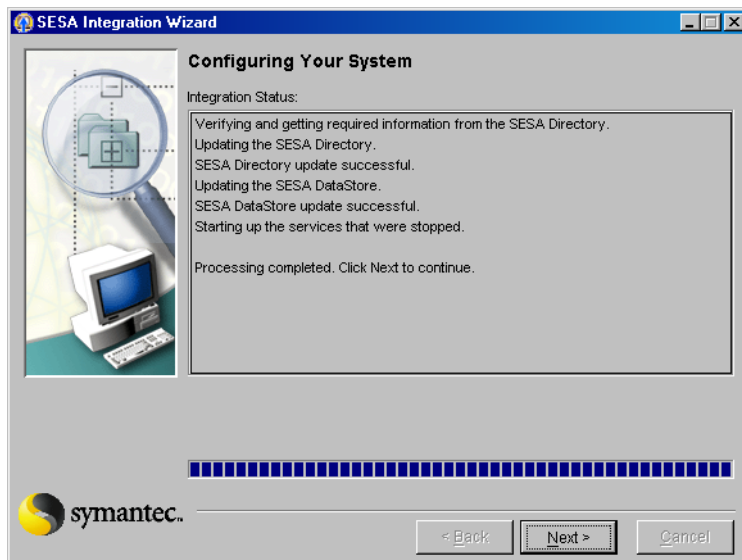
For more information on the SESA default, anonymous SSL, and upgrading to authenticated SSL, see the *Symantec Enterprise Security Architecture Installation Guide*.

Secure Directory Port

Type the port number.

The typical directory port number is 636.

- 7 Click **Next**.
- 8 In the Ready to proceed panel, do one of the following:
 - To change your settings, click **Back**.
 - To proceed, click **Next**.



In the Configuring Your System panel, the Integration Status window shows the progress of the installation.

This process may take several minutes.

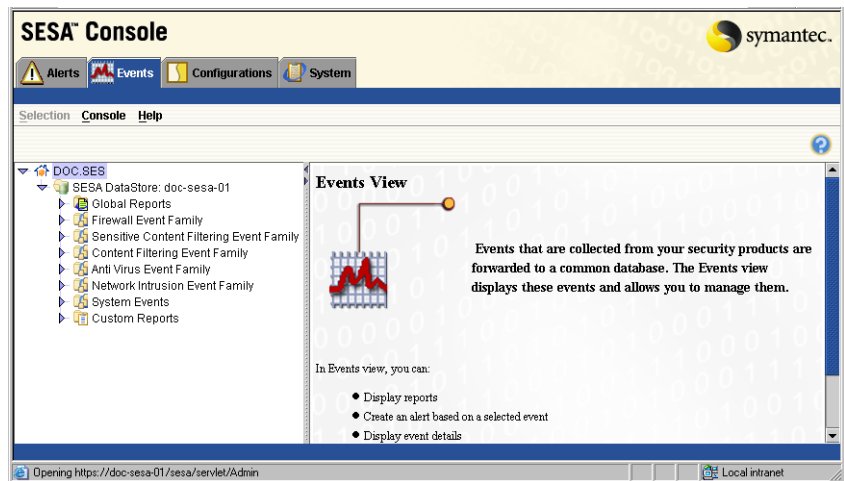
- 9 When the Processing completed message appears at the bottom of the window, click **Next**.
- 10 In the SESA Integration Successful panel, click **Finish**.

Verifying the Symantec Event Manager installation

To verify the installation, confirm that Security Gateways (Group 1) appears in the Configurations view tab of the SESA Console.

To verify the Symantec Event Manager installation

- 1 To display the SESA Console, do one of the following:
 - If you are working on the SESA Manager computer, on the Windows taskbar, click **Start > Programs > Symantec Enterprise Security > SESA Console**.
 - If you are not working directly on the SESA Manager computer, in a browser window type the URL of the SESA Manager.
- 2 Log on to the SESA Console using the Domain Administrator account.
- 3 In the SESA Console, on the Configuration view tab, in the left pane, confirm that Security Gateways (Group 1) is one of the listed products.
- 4 On the Event view tab, in the left pane, confirm that the following event families are listed: Firewall, Sensitive Content Filtering, Content Filtering, Antivirus, Network Intrusion.



Upgrading from Symantec Event Manager for Security Gateways v2.0 to Symantec Event Manager for Security Gateways v2.0.1

If you are already running Symantec Event Manager for Security Gateways (Group 1) v2.0 to centrally view events from Symantec security gateway appliances, you can upgrade to Symantec Event Manager for Security Gateways (Group 1) v2.0.1 without uninstalling.

To upgrade from Symantec Event Manager for Security Gateways v2.0

- 1 Back up your SESA Directory.
See the section on archiving a SESA Directory in the *Symantec Enterprise Security Architecture Installation Guide*.
- 2 Back up your SESA DataStore.
See the following Symantec Knowledge Base article for back up instructions:
<http://service1.symantec.com/SUPPORT/ent-gate.nsf/docid/2003042816055954>
This article, “How to migrate a SESA DB2 DataStore to a different computer”, describes the back up and restore process.
- 3 Perform the installation procedure that is described in “[Installing Symantec Event Manager for Security Gateways](#)” on page 76

You can also upgrade to Symantec Advanced Manager for Security Gateways (Group 1) v2.0.1. This upgrade gives you the added ability to manage your security gateway configurations through the SESA Console. See “[Upgrading from Symantec Event Manager for Security Gateways v2.0 to Symantec Advanced Manager for Security Gateways V2.0.1](#)” on page 68.

Uninstalling Symantec Event Manager

Before uninstalling, ensure that the SESA Manager is running on this system. The SESA Manager must be operating properly before you uninstall any SESA components.

Also, before you begin, obtain the following information from your SESA administrator:

- SESA Domain Administrator Name
- SESA Domain Administrator Password

- Host Name or IP Address of the SESA Directory
- Secure Directory Port

To uninstall the Symantec Event Manager for Security Gateways

- 1 Insert the *Symantec Event Manager for Security Gateways (Group 1) v 2.0.1* CD-ROM into the CD-ROM drive on the SESA Manager computer.
- 2 Browse to SESA/SIPI/, and then double-click **uninstall.bat**.
A command window shows the preparations for the uninstall procedure, followed by the Welcome dialog box.
- 3 In the Welcome to SESA Integration Wizard panel, click **Next**.
- 4 In the SESA Integration Requirements panel, click **Next**.
- 5 In the SESA Domain Administrator Information panel, do the following:

SESA Domain Administrator Name	Type the domain administrator's user name.
--------------------------------	--

SESA Domain Administrator Password	Type the domain administrator's password.
------------------------------------	---

Host Name or IP Address of SESA Directory	Type one of the following: ■ If SESA is using default, anonymous SSL communications, the IP address of the computer on which the SESA Directory is installed (it may be the same as the SESA Manager IP address if they are both installed on the same computer). You can also type localhost. ■ If SESA is using authenticated SSL communication, the host name of the SESA Directory computer. For example, mycomputer.com.
---	---

For more information on the SESA default, anonymous SSL, and upgrading to authenticated SSL, see the *Symantec Enterprise Security Architecture Installation Guide*.

Secure Directory Port	Type the port number. The typical directory port number is 636.
-----------------------	---

- 6 Click **Next**.

- 7 In the Ready to proceed panel, do one of the following:

- To change your settings, click **Back**.
- To proceed, click **Next**.

In the Configuring Your System panel, the Integration Status window shows the progress of the removal of Symantec Event Manager.

This process may take several minutes.

- 8 When the Processing completed message appears at the bottom of the window, click **Next**.
- 9 In the SESA Integration Successful panel, click **Finish**.

Joining security gateways to SESA

This chapter includes the following topics:

- [About joining SESA](#)
- [Preparing to join SESA](#)
- [Joining SESA](#)
- [Logging on to the SESA Console](#)
- [Troubleshooting problems when joining SESA](#)
- [Returning to local management](#)

About joining SESA

To join SESA, you run the Join SESA Wizard on the local security gateway, using the Security Gateway Management Interface (SGMI). The Join SESA Wizard runs on the connecting security gateway only. As the local administrator, you must also have administrative privileges on the SESA Manager to use the Join SESA Wizard.

Note: The procedures for connecting your existing stand-alone or clustered security gateways to the SESA Manager assume that the SESA environment is established, and that your security gateways are already configured.

The Join SESA Wizard performs the following tasks:

- Installs the SESA Agent on the security gateway.
The SESA Manager requires that each connecting security gateway have a SESA Agent running.
- Registers the SESA Agent with the SESA Manager.
- Exports local configuration to the SESA Manager, if you select that option.
- Instructs the SESA Manager to associate the exported configuration with the local security gateway.
- Validates the local policy and location settings if they are being exported to the SESA Manager.
- Downloads policy and location settings associated with an organizational unit if you select that option.
- Instructs the SESA Manager to assign the validated configuration with the local security gateway.

Instructions for joining SESA are also provided in the following:

- *Symantec Enterprise Firewall Administrator's Guide*, the *Symantec Gateway Security 5400 Series Administrator's Guide*
- *Symantec Advanced Manager for Security Gateways (Group1) and Symantec Event Manager for Security Gateways (Group1) Administrator's Guide*.

They are mirrored here so that SESA administrators can assist you in joining SESA.

Preparing to join SESA

Before you join a security gateway to SESA, you must ensure that the required software is installed and configured.

- On the SESA Manager, install either the Symantec Advanced Manager for Security Gateways (for both configuration management and event management) or the Symantec Event Manager for Security Gateways (for event management only).
See [“Installing Symantec Advanced Manager for Security Gateways”](#) on page 64 or [“Installing Symantec Event Manager for Security Gateways”](#) on page 76.
- Ensure that the security gateways that you want to manage or from which you want to collect events are installed.

- Configure each local security gateway.
- If you are joining multiple security gateways for centralized management, ensure that the network topology of all the security gateways is parallel.

Configuring the local security gateway

To prepare to join a security gateway to SESA, you must do the following:

- Configure your security gateway.
 At a minimum, you must run the System Setup Wizard to complete the initial setup of your system interfaces.
 You can also configure the security gateway's policy and location settings. If you configure the local security gateway, you can export these settings as your initial configuration for management in SESA. For the easiest transition to advanced management, you should use this method.
 See ["Choosing your starting point"](#) on page 54.
- Apply all valid security gateway licenses.
 Symantec Advanced Manager requires that you remove the security gateway from the SESA environment in order to add or change security gateway licenses. If you add all security gateway licenses locally before you join SESA, it will save you time later.
- Configure local log settings.
 To get the level of reporting you want, you may need to configure SESA event gating on the security gateway. For example, some event manager reports are based on the statistics message, which is disabled by default. See ["SESA event gating"](#) on page 45, and the section on SESA event gating in the *Symantec Gateway Security 5400 Series Administrator's Guide* and the *Symantec Enterprise Firewall Administrator's Guide*.
- Back up your local configuration.

Joining multiple security gateways to SESA for centralized management

In some circumstances, you can join multiple security gateways to SESA and use a single configuration to manage all of them. This means that the policies and location settings are identical for all security gateways.

The following are examples of when you could use this process:

- A corporation has multiple security gateways at a specific geographical location. These security gateways cannot be clustered because they are not identical systems.
Configurations could include one primary security gateway and one backup, or two primaries and one backup. Identical configurations on both security gateways provide for redundancy so that the perimeter is not left insecure if the primary security gateway is not available.
- A corporation that uses SESA has a very large LAN or WAN, where identical subnet access is available by way of multiple security gateways.
This organization has a master DNS table that works across all security gateways.

If you are joining multiple security gateways for centralized management, you must meet these additional prerequisites:

- Ensure that the number of network interfaces is identical.
- Configure the logical network interfaces to be named the same on each security gateway.
Generally, policies reference logical network interface names, and if they do not match on each security gateway, the validation fails.
- Configure network entities the same.

If you are joining your security gateways for scalable management, you should also identify how your security gateways will be logically grouped (region, organization, and so on) and determine that they can share both the same policy and location settings.

See [“Planning for SESA integration”](#) on page 49.

Joining SESA

Joining SESA lets you configure your security gateways from the SESA Console.

Before you join SESA:

- Determine the join SESA option that you will use.
- For all options, contact your SESA administrator for the following information, which you will need to complete the wizard:
 - SESA Manager IP address or fully qualified domain name
 - Thumbprint of the SESA Manager’s certificate
 - SESA logon name
 - SESA password

Determining your options for joining SESA

There are multiple options for joining a security gateway to SESA. The option you use depends on the product that you have installed to integrate your security gateway with SESA, how you will manage the security gateway from SESA, and the part the security gateway plays in your overall security strategy.

Table 8-1 Options for joining SESA

Type of SESA management	Security Gateway configuration option	Description
Configuration and event management Requires Symantec Advanced Manager for Security Gateways.	Export Local Configuration and Associate with Firewall	When you join a single, non-clustered security gateway to SESA, this option pushes the security gateways policy and location settings to SESA, where they are automatically associated with the security gateway. You should use this option if you are new to security gateway management through SESA. See “Exporting the local security gateway configuration to SESA” on page 88.
	Use selected organizational unit configurations	This option lets you select an organizational unit and import the policy and location settings that are associated with it to the local security gateway. This overwrites the policy and location settings on the local security gateway. To use this option, your network resources must be parallel to those defined in the location settings you will import. See “Importing an existing policy and location settings from SESA” on page 91.
Cluster management Requires Symantec Advanced Manager for Security Gateways	Cluster Configuration panel	When you join a cluster member to SESA, this option lets you specify the organizational unit that will represent the cluster in SESA. The policy and location settings of the cluster member are automatically associated with the organizational unit. Other cluster members are automatically joined to SESA using the same organizational unit and configurations. See “Joining a cluster to SESA” on page 94.

Table 8-1 Options for joining SESA (Continued)

Type of SESA management	Security Gateway configuration option	Description
Event management only Use Symantec Event Manager for Security Gateways or Symantec Event Manager for Security Gateways	Not applicable. When you join SESA for event management only, you cannot configure the security gateway from SESA.	This option lets you join individual and clustered security gateways to SESA for event management. You use the SESA Console to view the events, and create alerts and reports. See “Joining SESA for event management only” on page 99.

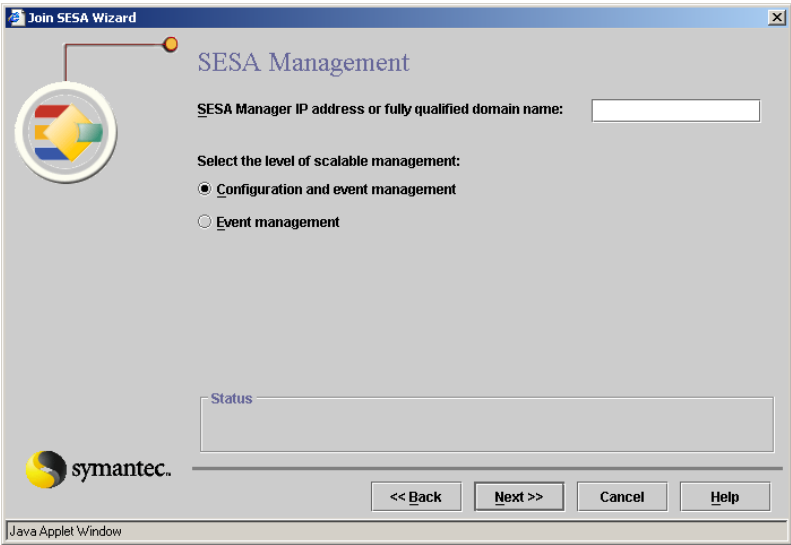
Exporting the local security gateway configuration to SESA

Use this procedure to join a single gateway to SESA and export its local configuration to SESA.

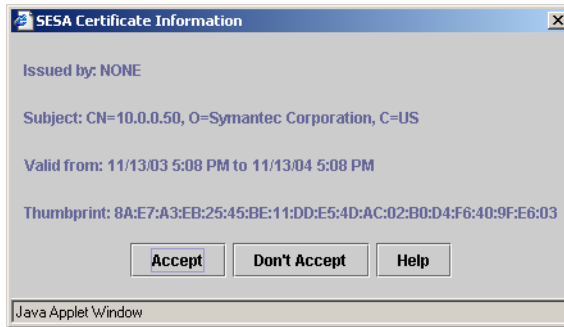
If you are new to using SESA to manage security gateways, this is the simplest way to connect a security gateway on the SESA Manager. It requires the least amount of preparation on the SESA Manager.

To export the local security gateway to SESA

- 1 In the Security Gateway Management Interface, on the Action menu, click **Scalable Management > SESA Setup**.
- 2 In the Welcome to Join SESA Wizard panel, click **Next**.

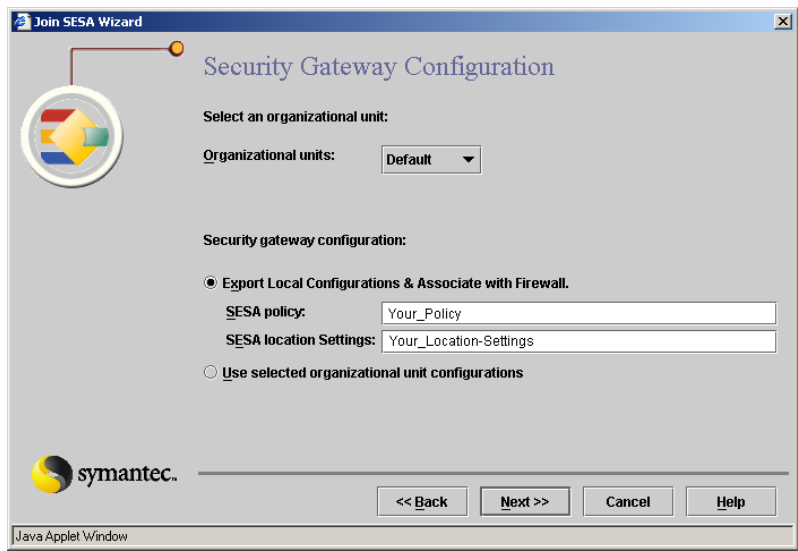


- 3 In the SESA Management panel, do the following:
 - In the SESA Manager IP Address text box, type the IP address or fully qualified domain name of the SESA Manager.
 - To manage your security gateway with SESA, click **Configuration and event management**.
 - Click **Next**.



- 4 In the SESA Certificate Information dialog box, do the following:
 - Verify that the certificate matches the thumbprint of the SESA Manager's certificate.
 - Click **Accept**.
- 5 In the SESA Log On dialog box, do the following:
 - In the Logon name text box, type your SESA logon name.
 - In the Password text box, type your SESA logon password.
- 6 Click **Next**.
 The wizard uses the SESA logon information to establish a session with the selected SESA Manager.

When the connection is established, the Security Gateway Configuration panel is displayed.

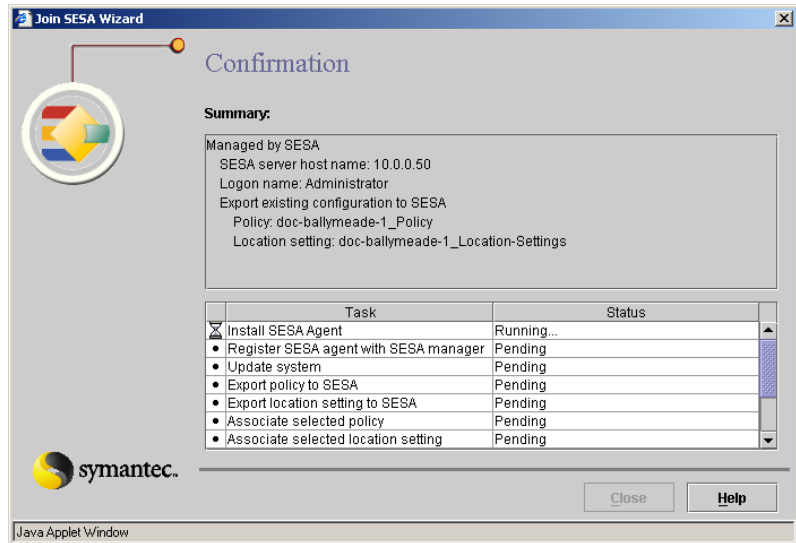


If the connection fails, the wizard prompts you again for the logon credentials. The wizard lets you try three times before aborting. If the login fails three times, you must run the wizard again to connect.

7 In the Security Gateway Configurations panel, do the following:

Organizational units	From the drop-down list, select an organizational unit. If no organizational units have been created in SESA, select Default or Managers.
Export Local Configuration and Associate with Firewall	Select this option to export your local configuration to SESA.
SESA Policy	Type a unique name under which your local policy will be stored in SESA. Spaces are not allowed. If you enter a name that is already in use, you are warned of the conflict.
SESA Location Settings	Type a unique name under which your local location settings will be stored in SESA. Spaces are not allowed. If you enter a name that is already in use, you are warned of the conflict.

- 8 Click **Next**.
- 9 In the Confirmation panel, click **Finish**.



The Task and Status columns show the progress of the Join SESA Wizard. When all steps are completed, the Finish button changes to a Close button.

- 10 Click **Close**.

Importing an existing policy and location settings from SESA

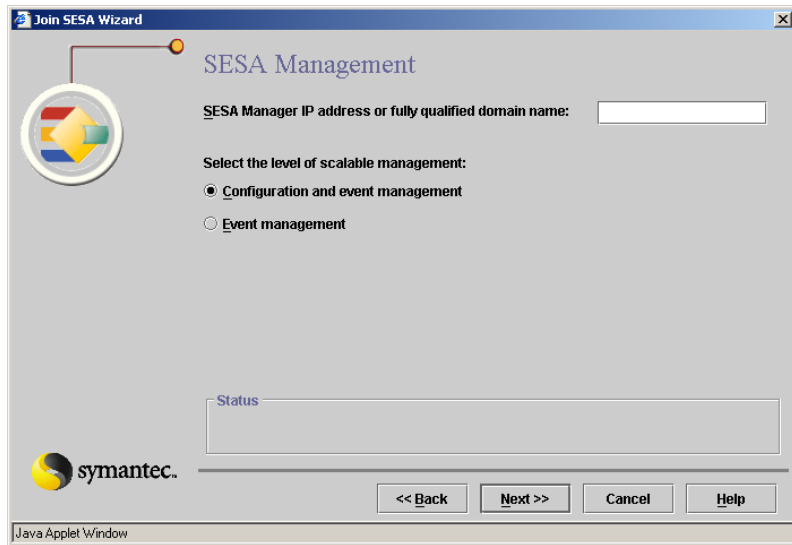
Use this procedure when you want the security gateway that you are joining to SESA to inherit the policy and location settings that are associated with an organizational unit in SESA.

To use this option, the network topology of the local security gateway must be parallel to the network topology represented by the location settings that are associated with the organizational unit.

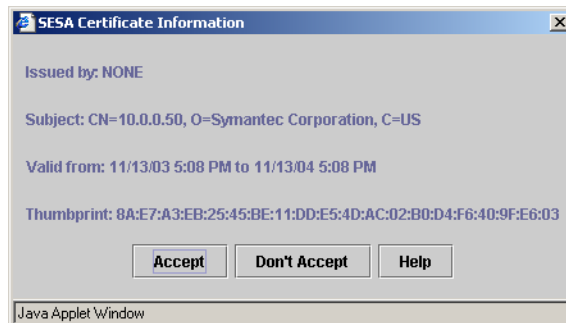
To import an existing policy and location settings from SESA

- 1 In the Security Gateway Management Interface, on the Action menu, click **Scalable Management > SESA Setup**.

- 2 In the Welcome to Join SESA Wizard panel, click **Next**.



- 3 In the SESA Management panel, do the following:
 - In the SESA Manager IP Address text box, type the IP address or fully qualified domain name of the SESA Manager.
 - To manage your security gateway with SESA, click **Configuration and event management**.
 - Click **Next**.



- 4 In the SESA Certificate Information dialog box, do the following:
 - Verify that the certificate matches the thumbprint of the SESA Manager's certificate.
 - Click **Accept**.

- 5 In the SESA Log On dialog box, do the following:
 - In the Logon name text box, type your SESA logon name.
 - In the Password text box, type your SESA logon password.
- 6 Click **Next**.
 The wizard uses the SESA logon information to establish a session with the selected SESA Manager.
 When the connection is established, the Security Gateway Configuration panel is displayed.



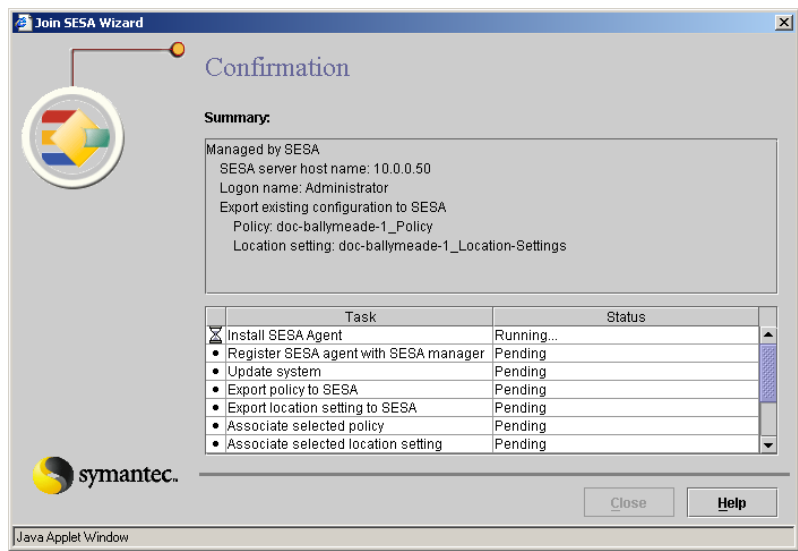
If the connection fails, the wizard prompts you again for the logon credentials. The wizard lets you try three times before aborting. If the login fails three times, you must run the wizard again to connect.

- 7 In the Security Gateway Configurations panel, do the following:

Organizational units	From the drop-down list, select the organizational unit from which you want to import the configuration.
Use selected organizational unit configuration	Select this option to import the policy and location settings that are associated with the organizational unit. Warning: Using an organizational unit's configuration overwrites your current policy and location settings on the local security gateway, including DNS settings.

- 8 Click **Next**.

9 In the Confirmation panel, click **Finish**.



The Task and Status columns show the progress of the Join SESA Wizard. When all steps are completed, the Finish button changes to a Close button.

10 Click **Close**.

Joining a cluster to SESA

Security gateway clusters are created locally by running the Cluster Wizard using SGMI. When you join a member of a cluster to SESA, you assign it to a single organizational unit. The cluster’s organizational unit name defaults to the local cluster name. All other members of the cluster are automatically joined to SESA when the first member joins.

The cluster behaves like any other organizational unit except that before you make any changes to its membership, the members of the cluster must leave SESA first. After the cluster members have left SESA, you can change cluster membership using the SGMI. Once the changes are made to the cluster membership, you can rejoin the cluster to SESA.

Join a cluster to SESA

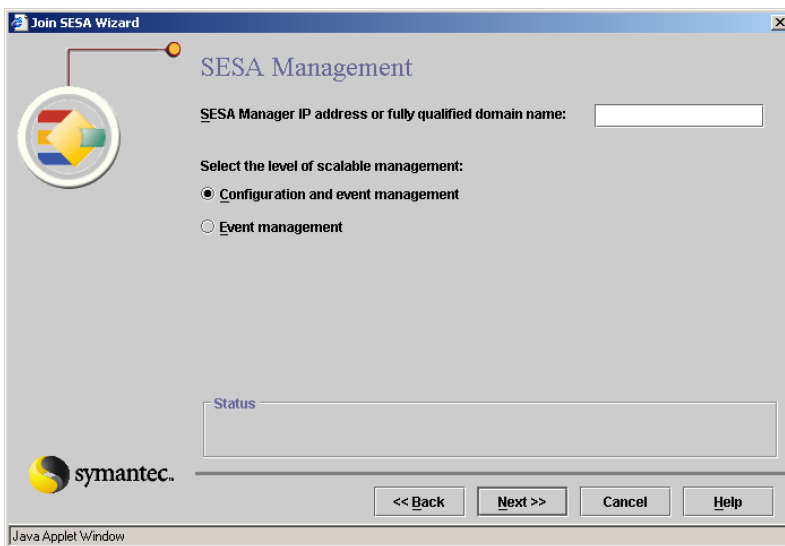
Joining a cluster member to SESA exports the cluster's policy and location settings to an organizational unit in SESA.

When a single node of the cluster joins SESA, all other nodes in the cluster automatically join and inherit the policy and location settings that are associated with the organizational unit.

After you join a cluster to SESA, you can change the organizational unit to which the cluster members belong.

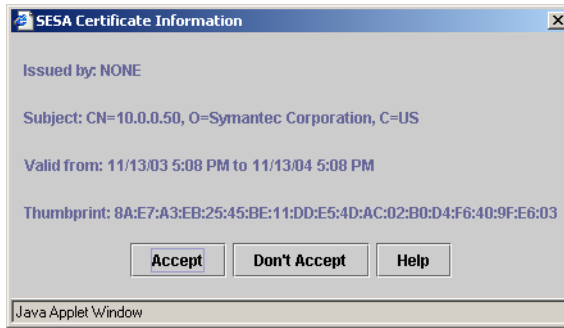
To join a cluster to SESA

- 1 In the Security Gateway Management Interface, on the Action menu, click **Scalable Management > SESA Setup**.
- 2 In the Welcome to Join SESA Wizard panel, click **Next**.



- 3 In the SESA Management panel, do the following:
 - In the SESA Manager IP Address text box, type the IP address or fully qualified domain name of the SESA Manager.
 - To manage your cluster with SESA, click **Configuration and event management**.

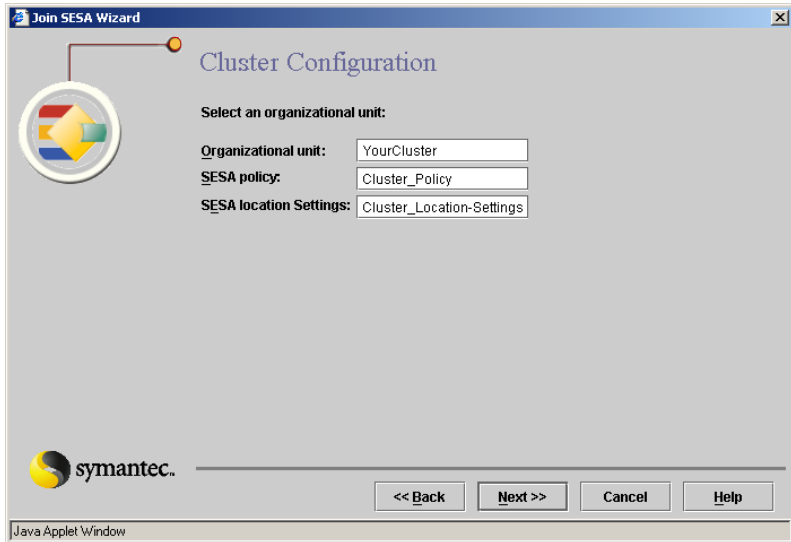
- Click **Next**.



- 4 In the SESA Certificate Information dialog box, do the following:
 - Verify that the certificate matches the thumbprint of the SESA Manager's certificate.
 - Click **Accept**.
- 5 In the SESA Log On dialog box, do the following:
 - In the Logon name text box, type your SESA logon name.
 - In the Password text box, type your SESA logon password.
- 6 Click **Next**.

The wizard uses the SESA logon information to establish a session with the selected SESA Manager.

If the connection fails, the wizard prompts you again for the logon credentials. The wizard lets you try three times before aborting. If the logon fails three times, you must run the wizard again to connect.



7 In the Cluster Configurations panel, do the following:

- | | |
|------------------------|---|
| Organizational unit | Specifies the name of the cluster, based on the current name of the cluster.

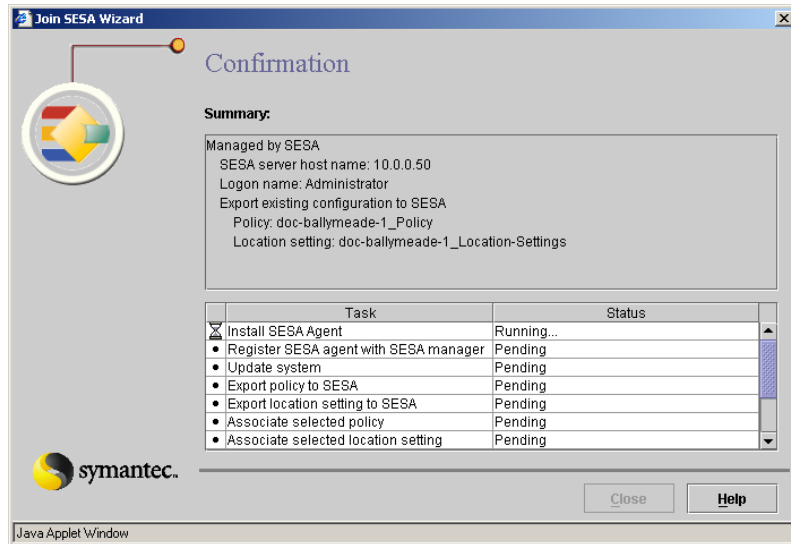
You can specify another name |
| SESA Policy | Type a unique name under which the cluster policy will be stored in SESA.

Spaces are not allowed. If you enter a name that is already in use, you are warned of the conflict. |
| SESA Location Settings | Type a unique name under which the cluster location settings will be stored in SESA.

Spaces are not allowed. If you enter a name that is already in use, you are warned of the conflict. |

8 Click **Next**.

- 9 In the Confirmation panel, click **Finish**.



The Task and Status columns show the progress of the Join SESA Wizard. When all steps are completed, the Finish button changes to a Close button.

- 10 Click **Close**.

To change the name of the cluster's organizational unit after you join SESA

- 1 In the SESA Console, on the System view tab, create a new organizational unit.
- 2 On the Configuration view tab, right click **Security gateways (Group 1)** and then click **Show All Gateways**.
- 3 In the Show All Gateways dialog box, on the Organizational Units tab, select the new organizational unit, and then click **Associate**.
- 4 Use the Associate Wizard to associate the policy and location settings of the old organizational unit with the new organizational unit.
- 5 On the System view tab, move the computers that represent the cluster members to the new organizational unit.

Joining SESA for event management only

Use this procedure if you want to join a single security gateway or a cluster of security gateways to SESA for the purpose of logging and reporting events only.

The security gateway machines are added to the Default organizational unit.

To join SESA for event management only

- 1 On the Security Gateway Management Interface Action menu, click **Scalable Management** > **SESA Setup**.
- 2 In the Welcome to Join SESA Wizard panel, click **Next**.
- 3 In the SESA Management panel, do the following:
 - In the SESA Manager IP Address text box, type the IP address or fully qualified domain name of your SESA Manager.
 - Click **Event management**.
 - Click **Next**.
- 4 In the SESA Certificate Information dialog box, do the following:
 - Verify that the certificate matches the thumbprint of the SESA Manager's certificate.
 - Click **Accept**.
- 5 In the SESA Log On dialog box, do the following:
 - In the Logon name text box, type the SESA administrator's user name.
 - In the Password text box, type the SESA administrator's password.
 - Click **Next**.
- 6 In the Confirmation panel, review the information, and then click **Finish**. The Task and Status columns show the progress of the Join SESA Wizard. When the SESA Agent has finished installing, the Finish button changes to a Close button.
- 7 Click **Close**.

Logging on to the SESA Console

Once your security gateway joins SESA, you log on to the SESA Console to begin managing the security gateway.

To log on to the SESA Console

- 1 On your local security gateway system, or on the SESA Manager, open a browser window.
- 2 Browse to **https://<SESA manager IP address or domain name>/sesa/ssmc** where <SESA manager IP address or domain name> is the IP address or fully qualified domain name of your SESA manager.
- 3 In the Logon name text box, type the SESA administrator's user name.
- 4 In the Password text box, type the SESA administrator's password.
- 5 Click **Log On**.

Troubleshooting problems when joining SESA

If the Join SESA Wizard fails, verify the following:

- Your information for connecting to SESA is correct.
 - IP address or domain name for the SESA Manager
 - SESA administrator user name and password
- You followed the appropriate scenario for the software you purchased. For example, if you purchased Symantec Event Manager only, you cannot join for Symantec Advanced Manager.
- If you are importing configurations, ensure that the location settings of your local security gateway are consistent with the location settings you are importing.

If you join SESA by importing an existing configuration, the network topology of your local security gateway must be parallel to the network topology that is represented by the location settings of the imported configuration.

When there is disparity, you can view the validation report in SESA to identify adjustments you must make so that the imported location settings work correctly with your security gateway.

In rare cases, the Join SESA Wizard succeeds but the security gateway does not appear to be joined to SESA. If either of the following occurs, reboot the local security gateway machine:

- If you log on to the SESA Console and do not see the security gateway as joined.
- If, in the SGMI, the homepage does not indicate that the security gateway has joined.

Returning to local management

You must manage some aspects of security gateways locally. These include:

- Changing system settings such as network interfaces
- Installing security gateway licenses
- Joining new members to a cluster
- For Symantec Gateway Security 5400 appliances, changing hardware settings and making feature choices
- For Symantec Enterprise Firewall 8.0, uninstalling the firewall
- Backing up your security gateway

To make these local changes, you must return the security gateway to local management.

Return to local management

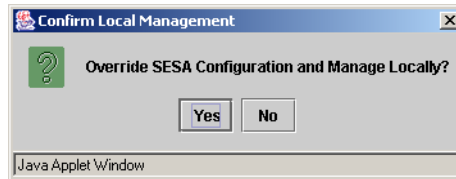
In the SGMI, two options on the Action menu, under Scalable Management, let you return to local management of your security gateway. Other options let you return to managing your security gateways from SESA.

Table 8-2 Options to return to local security gateway management

Option to manage locally	Reason to use	Option to return to SESA management
Local management	Temporarily return to local management to make local changes.	SESA Management
Leave SESA	Completely remove the registration of the security gateway from SESA.	SESA Setup (runs the Join SESA Wizard)

To return to local management temporarily

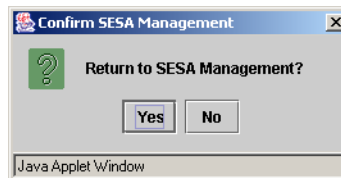
- 1 On the local security gateway, in the Security Gateway Management Interface (SGMI), on the Action Menu, select **Scalable Management > Local management**.



- 2 In the Confirm Local Management dialog box, do one of the following:
 - To overwrite the configuration that is being managed in SESA and manage your policy and location settings locally, click **Yes**.
 - To remain joined to SESA for configuration management, click **No**.

To return to SESA management after leaving temporarily

- 1 In the SGMI, on the Action Menu, select **Scalable Management > SESA management**.



- 2 In the Confirm Local Management message box, do one of the following:
 - To return to SESA management, click **Yes**.
 - To continue managing your security gateway locally, click **No**.

To return to local management permanently

- 1 In the SGMI, on the Action Menu, select **Scalable Management > Leave SESA Management**.
- 2 In the Leave SESA dialog box, do the following:

Ligon Name	Type the SESA administrator's user name.
Password	Type the SESA administrator's password.

- 3 Click **OK**.

- 4 If the local security gateway is a member of a cluster, do the following:
 - In the SESA Console, on the System view tab, expand Organizational Units.
 - Select the organizational unit that represented the cluster.
 - On the Selection menu, click **Delete**.
 - When you are prompted to confirm the deletion, click **Yes**.

To return to SESA management after leaving permanently

- 1 In the SGML, on the Action menu, click **Scalable Management > SESA Setup**.
- 2 In the Join SESA Wizard, choose the appropriate option for joining SESA, as described in [“Joining SESA”](#) on page 86.

Symantec Event Manager for Firewall (legacy products)

This section includes the following topics:

- [Introducing Symantec Event Manager for Firewall \(legacy products\)](#)
- [Remote Log utility](#)
- [Installing Symantec Event Manager for Firewall](#)
- [Verifying Symantec Event Manager for Firewall installation](#)

Introducing Symantec Event Manager for Firewall (legacy products)

This chapter includes the following topics:

- [Using Symantec Event Manager for Firewall with legacy products and security gateways](#)
- [How Symantec Event Manager for Firewall works](#)
- [Symantec Event Manager for Firewall components](#)

Note: The topics discussed in this chapter apply to Symantec Event Manager for Firewall only. For more information on Symantec Event Manager for Security Gateways, See [“Event management concepts”](#) on page 41.

Using Symantec Event Manager for Firewall with legacy products and security gateways

Symantec Event Manager for Security Gateways can report events from your legacy Symantec security gateways and third-party products (with separate purchase).

Symantec Event Manager for Firewall is required to collect events from:

- Symantec Gateways Security v1.0 appliances
- Symantec Enterprise Firewall v7.0.x
- VelociRaptor v1.5
- Third-party security gateways

How you install the components that integrate Symantec Event Manager for Firewall depends on the combination of products from which you want to collect events, and whether they are already managed by Symantec Event Manager for Firewall or Symantec Event Manager for Security Gateways.

See [“Determining installation options and order”](#) on page 56.

How Symantec Event Manager for Firewall works

Symantec Event Manager for Firewall components work together to collect and route log messages from one or more supported security gateway products to SESA. This enables centralized event logging, alerting, and reporting.

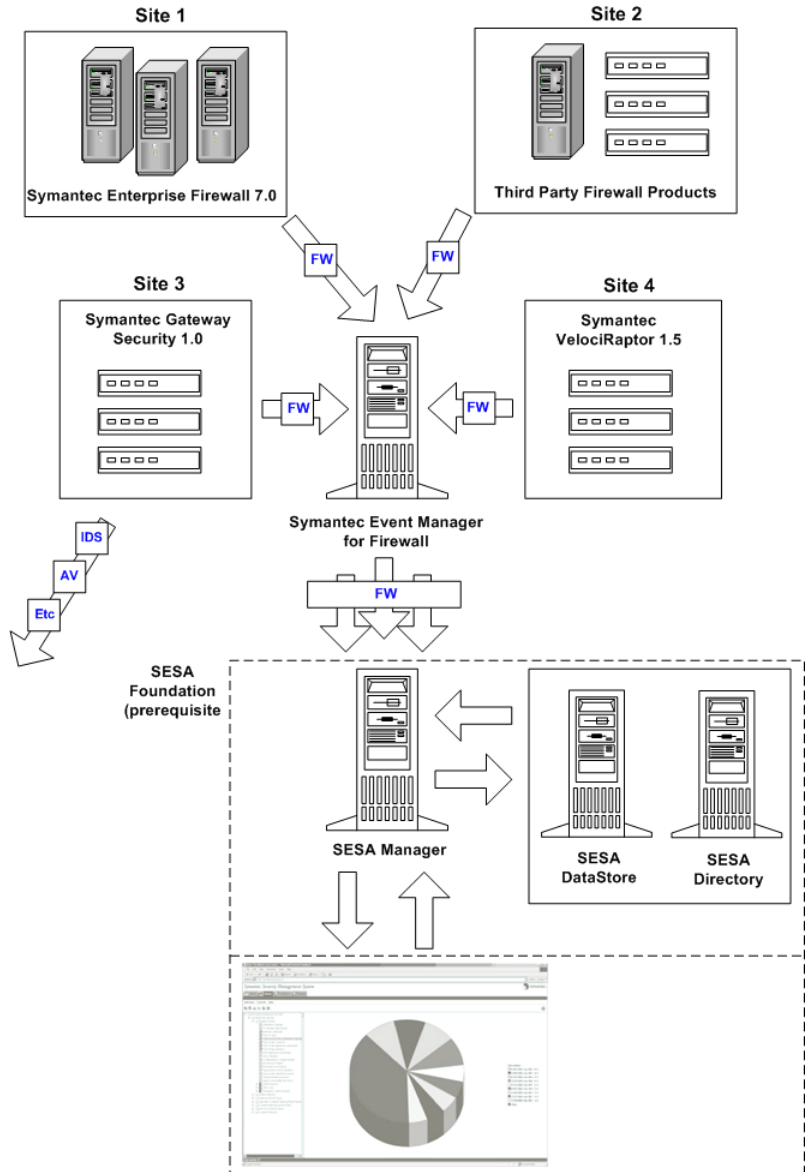
The Symantec Event Manager for Firewall allows event collection and routing to the SESA Manager to occur with minimal impact to your network operations.

To ensure the highest possible throughput, statistical event reporting is disabled initially when the Symantec Event Manager for Firewall is installed. If you want statistical reporting, you can easily enable it by changing a parameter setting in one of the Event Collector configuration files. See the section on customizing the Symantec Event Manager for Firewall in the *Symantec Advanced Manager for Security Gateways (Group 1) V2.0.1 and Symantec Event Manager for Security Gateways (Group 1) V2.0.1 Administrator’s Guide*.

The Symantec Event Manager for Firewall relies on the SESA components to transform data from firewall deployments across the enterprise into actionable security information, helping to reduce information clutter and improve your overall security posture.

Figure 9-1 shows the relationship between the Symantec Event Manager for Firewall and the SESA components (SESA Manager, SESA DataStore, and the SESA Directory).

Figure 9-1 Overview of Symantec Event Manager for Firewall data collection



Symantec Event Manager for Firewall components

Symantec Event Manager for Firewall installs shared and product-specific components that enable a supported security product to forward events to SESA.

- SESA integration components
- Symantec Event Manager for Firewall and the SESA Agent
- Event Collector for Symantec Security Gateways

These components are installed on the SESA Manager and on the remote log server that collects your firewall events.

Note: The use of a log server may not be required for third-party products. See your third-party documentation for specific installation details.

SESA integration components

To forward firewall events to SESA, you must extend SESA functionality to use the Event Collector data for Symantec or third-party security gateways. To do this, you install SESA integration components on the SESA Manager computer.

Integration with SESA is provided by the Symantec Event Manager for Security Gateways (Group 1) v2.0.1 or Symantec Advanced Manager for Security Gateways (Group 1) v 2.0.1.

The SESA integration components extend the tables and fields in the SESA DataStore so that they are prepared to accept 7.0.x Symantec security gateway data. You can centrally view the firewall events in a variety of report formats using the SESA Console.

How the Event Collector retrieves data

You install the Event Collector for Symantec Security Gateways and SESA Agent on a log server that is dedicated to event logging. This computer can be running either of the following operating systems:

- Microsoft Windows 2000 (Server and Advanced Server - Service Pack 3)
- Solaris 8 (32-bit or 64-bit)

You configure the log server with the IP address of each security gateway to which it will connect, and a shared password granting the log server permission to connect to the security gateway and obtain its log files.

When you install the Event Collector for Security Gateways, you provide the IP address of the first firewall to monitor, as well as the IP address of the SESA Manager, so that the SESA Agent knows with which SESA Manager it should communicate.

After you install the Event Collector for Symantec Security Gateways, it runs as a background service (on Microsoft Windows) or a daemon (on Solaris) that monitors log files for one or more remotely located security gateway products.

When you start remote logging, the Event Collector queries the log files, collects and formats events, and forwards them to the SESA Agent for logging to the SESA Manager.

How the Event Collector works with the SESA Agent

The Event Collector links to the SESA Agent, which securely logs the events that it receives to a SESA Manager on behalf of the Event Collector.

When product data or the SESA Agent is unavailable, the Event Collector sends error messages (for both Windows and Solaris) to a logs directory in C:\Program Files\Symantec\FWEventManager\Logs.

When the SESA Manager is unavailable, the SESA Agent queues messages for later delivery, up to a default maximum of 2 MB. You can change the queue size using the SESA Console. See the section on customizing the SESA Agent's Configuration in the *Symantec Advanced Manager for Security Gateways (Group 1) V2.0.1 and Symantec Event Manager for Security Gateways (Group 1) V2.0.1 Administrator's Guide*.

Note: If collecting event data from third-party security gateways, see the documentation that shipped with your Event Collector for the supported third party product.

How events are processed

In the SESA environment, events that arrive from a SESA Agent are generally understood to be events generated by the system on which the SESA Agent is installed.

In this application, however, the SESA Agent resides on the log server, which may receive events from multiple security gateway systems. To accommodate this, event data has been structured to uniquely identify the corresponding security gateway. The Event Collector logs security gateway events as if they originated with the firewall that first logged the message to the Event Collector.

See the appendix on events in the on *Symantec Advanced Manager for Security Gateways (Group 1) V2.0.1* and *Symantec Event Manager for Security Gateways (Group 1) V2.0.1 Administrator's Guide*.

Remote Log utility

This chapter includes the following topics:

- [About the Remote Log utility](#)
- [Enabling remote logging](#)
- [Installing the Remote Log utility on the log server](#)
- [Verifying remote logging operation](#)

Note: The topics discussed in this chapter apply to v7.0.x Symantec security gateways only.

For information on preparing a third-party security gateway for event collection using Symantec Event Manager for Firewall, see the documentation for the third-party collector.

About the Remote Log utility

Symantec Security Gateways include a remote logging utility that is key to the successful operation of Symantec Event Manager for Firewall. This utility lets a remote computer, in this case the log server, connect to individual Symantec security gateways to obtain copies of log files.

For remote logging to work, you must do the following:

- Configure each Symantec Security Gateway to grant the log server permission to connect it and obtain its log files.
- Install and run the Remote Log utility on the log server.
The “clientrepass” installation program lets you add a new host configuration that configures the log server to access firewall log files.

After you install and configure the Remote Log utility as described in this chapter, it is managed as a service by the Event Manager for Firewall, and requires no user intervention.

Note: You must configure the Remote Log utility when monitoring legacy Symantec security gateways. Third-party security gateways do not use Symantec's Remote Log utility.

The Remote Log utility is provided on your Symantec security gateway product CD-ROM. If you cannot locate the CD-ROM, contact your local sales representative or Symantec Customer Support for assistance.

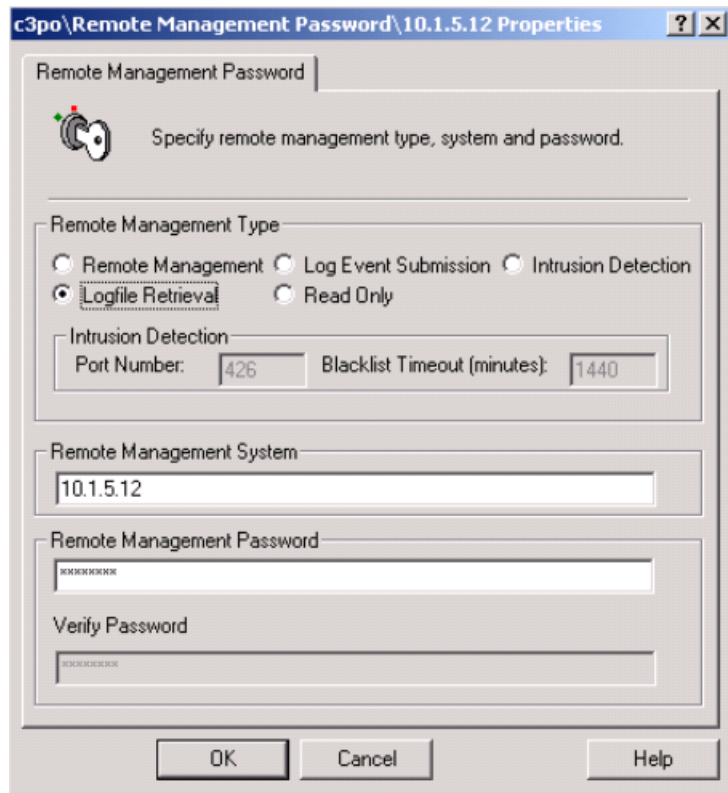
Enabling remote logging

To enable remote logging, you configure each Symantec Security Gateway to allow a remote connection. Use the Symantec Raptor Management Console (SRMC) to configure remote management information.

To enable remote logging on Symantec security gateways

- 1 On your desktop, double-click on the SRMC icon or select **Start > Programs > Symantec Raptor Management Console > Raptor Management Console**.
- 2 In the left pane, expand the **Symantec Enterprise Management** folder by clicking the icon or name.
- 3 Connect to a Symantec security gateway.
For details of connecting a security gateway, see your Symantec security gateway product documentation.
- 4 In the left pane, expand the **Base Components** folder.

- 5 Click **Remote Management Passwords**.



- 6 In the Remote Management Password Properties dialog box, on the Remote Management Password tab do the following:

Remote Management Type Select **Logfile Retrieval**.

Remote Management System	Type the IP address of the computer that acts as the remote log server. This is the computer on which the Event Manager for Firewall will be installed.
Remote Management Password	Type the password you require for the log server to be able to access the Symantec security gateway.
Verify Password	Verify the password you just typed in the text box above.

The password you enter here is the same password that you specify when you run the clientrempass installation program to configure the log server to access firewall log files.

See [“Installing the Remote Log utility on the log server”](#) on page 116.

- 7 Repeat steps 3 through 6 for each Symantec security gateway whose log files are monitored.
- 8 When done, in the SRMC main window, click **Save and Reconfigure**.
- 9 To close the SRMC, on the Console menu, click **Log Off**.

Installing the Remote Log utility on the log server

This section describes how to install the Symantec Security Gateway’s Remote Log utility on the log server. It also describes how to run the clientrempass program to enable the log server to access firewall log files.

The self-extracting files rlog_7-winnt.exe, and rlog_7-solaris.tar are located on the SEF or SEVPN CD-ROM in the ClientSoftware\Remotelogs\3DES or DES directory. Use the appropriate file for Microsoft Windows or Sun Solaris 7 or 8.

To configure the log server

- 1 Create a directory on the log server hard drive (for example RemoteLog), where you want to extract the Remote Log utility.
- 2 Insert the Symantec Enterprise Firewall or Symantec Enterprise VPN distribution CD-ROM into the CD drive on the log server.
- 3 Navigate to the ClientSoftware\Remotelogs\3DES or DES directory and copy the rlog_7-winnt.exe or rlog_7-solaris.tar file to the directory that you created in step 1.
- 4 Start the self-extracting executable file by doing one of the following:
 - In Windows, double-click on rlog_7-winnt.exe.
 - In Solaris, type:
`./rlog_7-solaris.tar`
- 5 Follow the prompts to unzip the files.
- 6 When done, start clientrempass by doing the following:
 - In Microsoft Windows, double-click on clientrempass.exe.
 - In Solaris, type:
`./clientrempass`

The following text appears in the terminal window:

```
REMPASS - Host, password, service, and port configuration tool
-----
Enter one of the Rempass options shown below:

(A)dd new Host Configuration
(C)hange existing Host Configuration
(D)elete existing Host Configuration
(L)ist existing Rempass Host entries
(Q)uit Rempass
```

Rempass Option:

- 7 At the Rempass Option prompt, to add a new host configuration, type **a**, and then press **Enter**.
- 8 At the Host name or IP address prompt, type the host name or IP address of the Symantec security gateway, and then press **Enter**.

The following service list is displayed:

Service List:

```
(1) Logfile Retrieval
    -Configure this client to access firewall logfiles
(2) Log Event Submission
    - Configure this client to submit events to firewall log
(3) Content Scanning
    - Configure content scanner for use by firewall
```

Please Choose a Service ('m' for main menu):

- 9 When prompted to choose from the Service List, to select Logfile Retrieval, type **1**.
- 10 At the Port Number prompt, type the port (on the firewall) through which the log server should connect.
To accept the default, 417, press **Enter**.
- 11 You are prompted to enter the passphrase for the security gateway that you identified in step 8:

```
Enter up to 64 characters for
192.168.10.2's passphrase
```

Type the same password here that you entered for the Symantec security gateway's remote management password (in the Remote Management Password Properties dialog box in the SRMC).

“See [“Enabling remote logging”](#) on page 114.”

- 12 Press **Enter**.
- 13 Verify the password by retyping it when prompted and then press **Enter**.
- 14 Repeat steps 7 through 13 for each Symantec Security Gateway.
- 15 When done, to quit clientrempass, press **Q**.

Verifying remote logging operation

To verify that the remote logging utility is working properly, view a remote log file for a Symantec security gateway from a command prompt on the log server.

To verify remote logging operation

- ◆ From the command prompt on the log server, type:
`remotelogfile <IP ADDRESS> logfile`
where <IP ADDRESS> is the IP address of the security gateway whose log file you want to view.

If remote logging is configured correctly on the security gateway and the log server, you should see the text of the remote log file scroll rapidly by on the log server's monitor.

If you receive an error, review the procedures in [“Enabling remote logging”](#) on page 114 and [“Installing the Remote Log utility on the log server”](#) on page 116 to verify remote logging configuration.

Installing Symantec Event Manager for Firewall

This chapter includes the following topics:

- [About Symantec Event Manager for Firewall installation](#)
- [Symantec Event Manager for Firewall components](#)
- [System requirements and setup](#)
- [Before you install](#)
- [Installing SESA integration components on the SESA Manager](#)
- [Upgrading from Symantec Event Manager for Firewall v1.0 to Symantec Event Manager for Security Gateways v2.0.1](#)
- [Configuring network interfaces and remote management hosts](#)
- [Customizing the SESA Agent's configuration](#)
- [Customizing the SESA Manager's configuration](#)
- [Configuring Symantec Event Manager for Firewall to monitor multiple Symantec Security Gateways](#)
- [Event Collector for Symantec Security Gateways service/daemon](#)
- [Managing disk space for log files](#)
- [Uninstalling the Event Collector for Symantec Security Gateways](#)

Note: The topics discussed in this chapter apply to Symantec Event Manager for Firewall only.

For information on Symantec Event Manager for Security Gateways, see [“Event management concepts”](#) on page 41 and [“Installing Symantec Event Manager for Security Gateways”](#) on page 73.

About Symantec Event Manager for Firewall installation

This chapter provides step-by-step instructions for installing Symantec Event Manager for Firewall to collect events from v7.0.x Symantec security gateways.

It includes procedures for a new installation and for upgrading from Symantec Event Manager for Firewall v1.1 to Symantec Event Manager for Security Gateways v2.0.1.

To collect event data from third-party security gateways, you must install the Symantec Event Collector for the third-party product (purchased separately). See the documentation shipped with your Event Collector for further information.

Symantec Event Manager for Firewall components

To use the Symantec Event Manager for Firewall to collect events, you install components on the following computers:

- The SESA Manager to which the security gateway events are forwarded
- One of the following:
 - For v7.0.x Symantec security gateways, the log server that collects log messages
 - For third-party security gateways, the security gateway that sends events

Table 11-1 describes each Symantec Event Manager for Firewall component, where it is installed, and the installation wizard that is used. (Installation wizards are located on the Symantec Event Manager for Security Gateways (Group 1) product CD-ROM.)

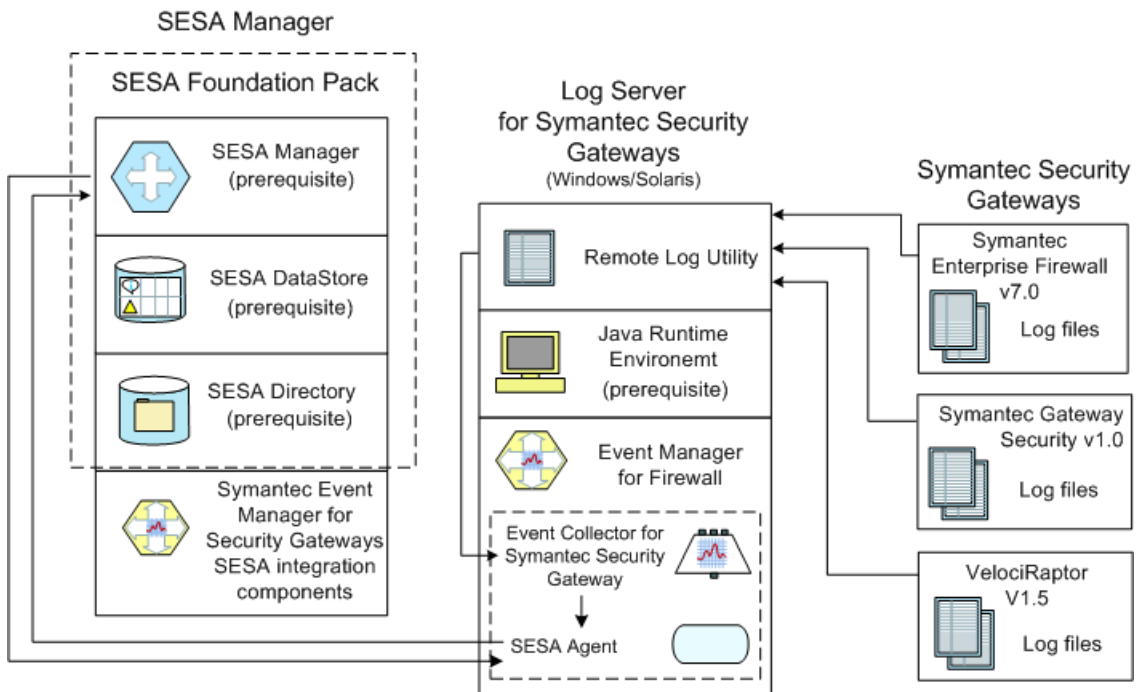
Table 11-1 Symantec Event Manager for Firewall components

Component	Installation location	Wizard	Where required
Symantec Event Manager for Security Gateways– SESA Integration components	SESA Manager computer	SESA Integration Wizard	Symantec and third-party security gateways
Symantec Event Manager for Firewall – SESA Agent	Symantec security gateway log server or third-party security gateway	Symantec Event Manager for Firewall InstallShield Wizard	Symantec and third-party security gateways

Table 11-1 Symantec Event Manager for Firewall components

Component	Installation location	Wizard	Where required
Symantec Event Manager for Firewall – Event Collector for Symantec Security Gateways	Symantec security gateway log server	Symantec Event Manager for Firewall InstallShield Wizard	Symantec security gateways

Figure 11-1 illustrates how the Symantec Event Manager for Firewall components work together to collect events from v7.0.x Symantec security gateways.

Figure 11-1 Symantec Event Manager for Firewall components


Note: You must install SESA Foundation Pack 1.1 before you begin installing the Symantec Event Manager for Firewall.

Before you install the Symantec Event Manager for Firewall components, perform the following tasks:

- Ensure connectivity between the SESA Manager and the log server where you will install the Symantec Event Manager for Security Gateways. See [“SESA Foundation requirements”](#) on page 123.
- On the SESA Manager, install the SESA integration components by installing either Symantec Event Manager for Security Gateways (Group 1) or Symantec Advanced Manager for Security Gateways (Group 1). See [“Installing Symantec Event Manager for Security Gateways”](#) on page 76 or [“Installing Symantec Advanced Manager for Security Gateways”](#) on page 64.

The descriptions in this chapter are based on installing Symantec Event Manager for Security Gateways.

Symantec Advanced Manager for Security Gateways is only required if you intend to manage v8.0 Symantec security gateways.

- On the log server, install the following:
 - Remote Log utility (only required for Symantec security gateways) [“Remote Log utility”](#) on page 113.
 - Java Runtime Environment (JRE) version 1.3.1_02
The JRE is a prerequisite for using the SESA Agent component of the Symantec Event Manager for Firewall.
See [“Installing the Java Runtime Environment”](#) on page 127.
 - Symantec Event Manager for Firewall–SESA Agent
The Symantec Event Manager for Firewall includes the SESA Agent that forwards events to the SESA Manager.
See [“Installing Symantec Event Manager for Firewall”](#) on page 128.
 - Symantec Event Manager for Firewall–Event Collector for Symantec Security Gateways
The Event Collector for Symantec Security Gateways collects events from Symantec Security Gateways and formats them for SESA.
See [“Installing Symantec Event Manager for Firewall”](#) on page 128.

System requirements and setup

Before installing Symantec Event Manager for Security Gateways, ensure that your environment and the computers on which you install Symantec Event Manager for Security Gateways meet the requirements described in this section.

SESA Foundation requirements

Ensure that the components of the SESA Foundation are installed and operating properly. For more information, see the *Symantec Enterprise Security Architecture Installation Guide*.

To verify connectivity between the log server and the SESA Manager, be aware of the following:

- By default, the SESA Agent connects to the SESA Manager using HTTPS on port 443. You can configure a different port if desired.
- To ensure that event messages reach the SESA Manager, appropriate routing must exist between the computer on which the Event Collector is installed and the SESA Manager.
- In addition, ensure that there is no firewall policy blocking the connection between the Event Collector and the SESA Manager.

To test for connectivity

- ◆ At a command prompt issue the following command:

```
telnet <SESA-IP-ADDRESS> 443
```

where <SESA-IP-ADDRESS> is the IP address of the SESA Manager.

SESA DataStore requirements

The SESA DataStore computer, installed during the SESA Foundation installation, must have enough hard disk space to accommodate the additional security events that Symantec or third-party security gateways will generate.

The amount of disk space you will need to accommodate the event data depends on how many devices are logging events, how verbose they are, and how long you want to keep the event data.

128 GB should be sufficient to store events from several firewalls for 30-days.

See [“Network sizing requirements for Symantec security gateways”](#) on page 125.

System requirements for the log server computer

You install the Symantec Event Manager for Firewall components on the computer you configure as the log server for your Symantec security gateways. The log server computer must meet the minimum system requirements listed in [Table 11-2](#).

Table 11-2 Requirements for the log server computer

Component	Description
Operating system	One of the following: ■ Microsoft Windows 2000 Server with Service Pack 3 or later ■ Microsoft Windows 2000 Advanced Server with Service Pack 3 or later ■ Solaris 8 (32-bit or 64-bit)
Sun Java requirements	■ Java Runtime Environment (JRE) version 1.3.1_02
Processor	■ Intel Pentium III-compatible 1 GHz processor (Windows) ■ Sun Microsystems sbus or PCI UltraSPARC workstation
Memory	■ 512 MB of memory for the SESA Agent and all Symantec security products (although 1 MB is recommended)
Hard disk space	■ 11 MB disk space for Event Collector and SESA Agent ■ 1 MB disk space for RemoteLog utility ■ 2 GB free disk space for RemoteLog files for each supported firewall
Network connection	■ TCP/IP connection to network

Network sizing requirements for Symantec security gateways

This section provides guidelines to help you determine the number of Symantec Event Manager for Firewalls, SESA Managers, and SESA DataStores you need to manage specific numbers of Symantec security gateways. Information in this section applies to Symantec security gateways only.

Note: Information in the [Table 11-3](#) was derived from a Symantec Security Gateway that generated a 200 MB log file per day. The information is intended to be a guideline only; the actual size of log files will vary depending on the size of your network and the amount of traffic generated.

Table 11-3 Symantec Event Manager for Firewall components

Symantec Security Gateways	Symantec Event Manager for Firewall	SESA Managers	SESA DataStores
25	1	1	1
50	2	2	1
100	4	3	2

For large organizations that manage more than 100 security gateways, the SESA implementation may require detailed planning to deploy. Contact your authorized sales representative or Symantec Systems Engineer for assistance in determining the appropriate sizing guidelines.

Before you install

Before you install Symantec Event Manager for Firewall, complete the following prerequisites:

- For all security gateways, ensure that the SESA Foundation is installed and operating properly. For more information, see *Symantec Enterprise Security Architecture Installation Guide*.
- Configure each security gateway to log normal activity. This ensures that all possible events are logged to SESA.
For v7.0.x Symantec security gateways, use the Symantec Raptor Management Console (SRMC) to ensure that the Log Normal Activity setting is enabled.
For more information, see *Symantec Enterprise Firewall and Symantec Enterprise VPN Configuration Guide*.

- For Symantec security gateways only, install and configure Remote Logging on the log server and each Symantec security gateway to be monitored.

Note: Third-party security gateways do not use Symantec's Remote Log utility.

See [“Remote Log utility”](#) on page 113.

- For all security gateways, install the Java Runtime Environment (JRE) version 1.3.1_02 on the log server, to support the installation of the SESA Agent.

If JRE is not already installed, you can obtain the JRE software from Sun's Web site at http://java.sun.com/products/archive/j2se/1.3.1_02/jre/index.html.

See [“Installing the Java Runtime Environment”](#) on page 127.

Installing SESA integration components on the SESA Manager

The first step in installing Symantec Event Manager for Firewall is to install the SESA integration components on the SESA Manager computer.

These components integrate Symantec or third-party security gateways with SESA by installing the firewall event schema into the SESA DataStore (database) and SESA Directory. This includes predefined reports for all firewall-related events (common reports for all supported security gateways, as well as product-specific reports for Symantec security gateways).

There are two scenarios:

- **Installing Symantec Event Manager for Firewall for the first time**
To install the SESA integration components, you install the Symantec Event Manager for Security Gateways (Group 1) or Symantec Advanced Manager for Security Gateways (Group 1), using a wizard that is supplied on the product CD-ROMs.
Follow the installation instructions in [“Installing Symantec Event Manager for Security Gateways”](#) on page 73 or [“Installing Symantec Advanced Manager for Security Gateways”](#) on page 61.
- **Upgrading from Symantec Event Manager for Firewall v1.0**
See [“Upgrading from Symantec Event Manager for Firewall v1.0 to Symantec Event Manager for Security Gateways v2.0.1”](#) on page 134.

Installing Symantec Event Manager for Firewall components on the log server

Install the following software on the log server that collects the v7.0.x Symantec security gateway events:

- JRE
- Symantec Event Manager for Firewall

Installing the Java Runtime Environment

The Java Runtime Environment (JRE) version 1.3.1_02 is required by the SESA Agent. If it is not already present on your system, you must install it before installing the Event Manager for Firewall (which includes the SESA Agent installation).

To install the Java Runtime Environment

First, determine if the JRE is already installed. If not, then you can install it on Windows or Solaris.

To determine whether the Java Runtime Environment is installed

- 1 Display a DOS prompt (for Windows), or a terminal window (for Solaris).
- 2 Type the following command:

```
java -version
```
- 3 Verify that the Java Runtime Environment is installed and that the Java version is 1.3.1_02.
- 4 If it is not, install the Java Runtime Environment before you install the Event Manager for Firewall.

To install the Java Runtime Environment

- 1 If you do not have JRE v 1.3.1_02 or later installed on your system, download the software from Sun's Web site at http://java.sun.com/products/archive/j2se/1.3.1_02/jre/index.html.
- 2 Start the installation by double-clicking on the downloaded executable.
- 3 Follow the installation instructions on the screens.

Installing Symantec Event Manager for Firewall

You install the Symantec Event Manager for Firewall components on a single log server that is dedicated to firewall event logging. This can be either a Microsoft Windows or Sun Solaris 8 computer that meets the minimum requirements described in [“System requirements for the log server computer”](#) on page 124.

You install the following components, using the Symantec Event Manager for Firewall InstallShield Wizard that is located on the *Symantec Event Manager for Security Gateways (Group 1)* CD-ROM:

- Event Manager for Firewall
- SESA Agent
- Event Collector for Symantec Security Gateways

How the installation proceeds depends on whether the SESA Agent is already installed on the log server. If not already installed, the SESA Agent is included as part of the Event Manager for Firewall installation. If it is already installed, the Event Manager for Firewall installation proceeds without installing the SESA Agent.

Note: Different settings are required when you install the Event Manager for Firewall to monitor third-party security gateways. For more information, see the documentation that is shipped with your third-party Event Collector.

Install Symantec Event Manager for Firewall

The log server computer can be running either of the following operating systems:

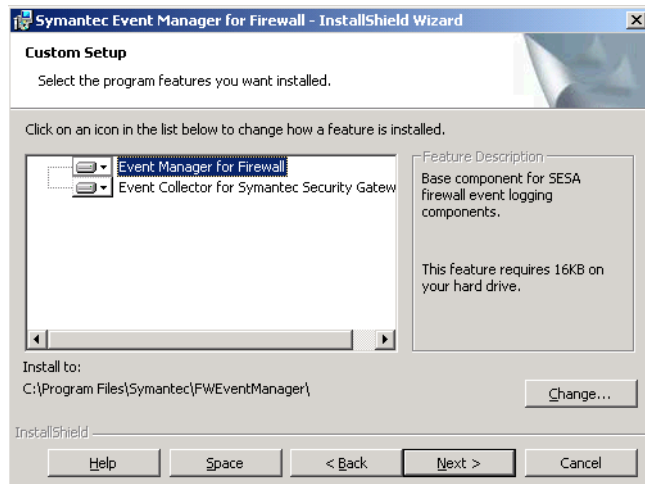
- Microsoft Windows
- Sun Solaris 8

The log server must meet the minimum requirements described in [“System requirements for the log server computer”](#) on page 124.

To install the Symantec Event Manager for Firewall, the SESA Agent, and Event Collector for Symantec Security Gateways on Microsoft Windows

- 1 Insert the *Symantec Event Manager for Security Gateways* CD into the CD-ROM drive on the log server.
- 2 Navigate to the following directory: EM_Firewall_1_0/Windows.
- 3 Double-click **setup.exe**.

- 4 In the Event Manager for Firewall InstallShield Wizard Welcome dialog box, click **Next**.
- 5 In the License Agreement dialog box, read the License Agreement and do one of the following:
 - Click **I accept the terms in the license agreement**, and then click **Next**.
 - Click **I do not accept the terms in the license agreement**.
This cancels the installation process.
- 6 If you are installing Symantec Event Manager for Firewall to monitor v7.0.x Symantec security gateways, in the Custom Setup panel, do not make any changes to the Event Manager for Firewall and Event Collector for Symantec Security Gateways settings.



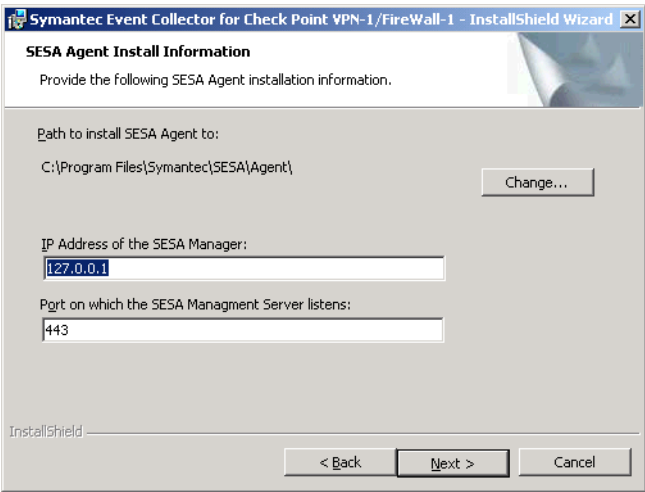
Do one of the following:

- To install to the default location, click **Next**.
The default location is
C:\Program Files\Symantec\FWEventManager\

- To change the default location, click **Change**.
In the Change Current Destination Folder dialog box, select a new location, click **OK**, and then click **Next**.

If the SESA Agent is not installed on your system, the SESA Agent Install Information panel is displayed.

If you do not see this panel, continue at step 11.



7 In the SESA Agent Install Information panel, do the following:

- | | |
|--------------------------------|---|
| Path to install SESA Agent to | To change the location where the SESA Agent is installed, click Change.

In the Change the SESA Agent Distribution Folder dialog box, specify the destination folder for the SESA Agent, and then click OK . |
| IP Address of the SESA Manager | Do one of the following: <ul style="list-style-type: none">■ If SESA is using default anonymous SSL, type the IP address of the SESA Manager computer.■ If SESA has been upgraded to use authenticated SSL, type the host name of the SESA Manager computer. |

8 Click **Next**.

9 In the Collector Information panel, do the following:

- | | |
|--|---|
| Enter the IP address of the first firewall to be monitored | Type the IP address for the first firewall that you want to monitor |
| Enter the path to the JRE directory | Type the path to where the JRE is installed on the log server. |
| Enter the full path (with filename) to the remotelogle utility | Type the full path, on the log server, where the RemoteLog Utility is installed |

10 Click **Next**.

11 In the Logfile Information panel, do the following:

- | | |
|--|--|
| Enter the filename of the logfile on the firewall | Type the name of the most current log file on the security gateway that you want the RemoteLog Utility to retrieve.

Note: In most cases, the file name is logfile unless it has specifically been changed. |
| Enter the directory in which to store the logfiles locally | Type the path (on the log server) where you want to store the security gateway's log file. |
| Enter the name of the initial local logfile copy to be created | Type the name you want to assign to the local copy of the log file. |
| Keep copies of logfiles on this system | If you want to archive log files, check here.

If you decide to archive log files, once the file reaches a maximum size of 50,000 events, new log files are automatically created in the directory specified above. |
| Enter the name of the alternate local logfile copy to be created | If you are not archiving log files, type the name you want to assign to the second (alternate) log file.

If you do not archive log files, the Event Collector will save events dynamically between two log files. Be sure to type a name for an alternate log file.

For more information, see “Managing disk space for log files” on page 145. |

12 Click **Next**.

13 In the Ready to Install the Program panel, click **Install**.

A DOS window shows the installation of files. When it closes, the Status field of the Installing Event Manager for Firewall dialog box shows the progress of the installation of the SESA Agent.

After the SESA Agent is installed, there is a pause, followed by the installation of the Event Collector for Symantec Security Gateways files.

14 In the InstallShield Wizard Completed panel, click **Finish**.

Before you use the Event Manager for Firewall, make sure it is properly installed by using the procedures in [“Verifying Symantec Event Manager for Firewall installation”](#) on page 149.

To start the Event Collector for Firewall, reboot your system.

To install the Symantec Event Manager for Firewall, the SESA Agent, and Event Collector for Symantec Security Gateways on a Solaris log server

1 Insert the *Symantec Event Manager for Security Gateways (Group 1)* product CD-ROM into the CD drive on the log server.

2 Change directory to:

```
cd /cdrom/cdrom0/EM_Firewall_1_0/Solaris
```

or as appropriate for your environment.

3 Execute the install program:

```
./install
```

The text of the license agreement appears.

4 To scroll through the license agreement, press **Enter**.

5 When you are prompted as to whether you accept the terms of the license agreement, do one of the following:

- To accept the agreement, type **y** (yes).

- To exit the installation process, type **n** (no).

The installation procedure continues to install the SESA Agent.

6 When prompted, type the IP address of the SESA Manager computer.

What is the SESA Manager IP or hostname? **10.1.5.6**

7 Next, type the IP address of the first firewall you want to monitor.

What is the first Firewall's IP address? **10.1.5.7**

8 Type the name of the log file on the security gateway that you want the RemoteLog Utility to retrieve.

What is the filename of the logfile on the firewall? **logfile**

- 9 When asked if the collector should archive the log files after processing them, type one of the following:
 - Y: The files are archived.
 If you decide to archive log files, once the file reaches a maximum size of 50,000 events, new log files are automatically created in the directory specified in step 11.
 - N: The files are not archived.
 If you do not archive log files, the Event Collector will save events dynamically between two log files. Be sure to type a name for an alternate log file in step 13.

See [“Managing disk space for log files”](#) on page 145.
- 10 Type the path (on the log server) where you want to store the security gateway’s log file (the default is /usr/raptor/bin).

What is the path in which to store the local logfile(s) (do not include the filename)? **/sef**
- 11 When prompted, type the name of the file that is used as the initial local copy of the logfile.

What is the name to use for the initial local copy of the logfile? **logfile**

If you chose to not archive log files (in step 9), the Event Collector saves events dynamically between two log files.
- 12 When prompted, type the name you want to assign to the second (alternate) log file.

The collector will alternate between two local files for capturing the firewall's logfile. What is the alternate filename to use for the local copy of the logfile? **logfile1**

For more information, see [“Managing disk space for log files”](#) on page 145.
- 13 Type the path to where the JRE is installed on the log server.

What is the path to the Java Run-time (do not include the 'bin' directory)? **/usr/j2re1_3_1_02**
- 14 Type the full path (with no extra spaces), on the log server, where the RemoteLog Utility is installed.

What is the full path to the remotelogfile utility (including the filename)? **/sef/remotelogfile**

The installation program installs the Symantec Event Manager for Firewall and Event Collector for Symantec Security Gateways.
- 15 Before using the Event Manager for Firewall, make sure it is properly installed, using the procedures in [“Verifying Symantec Event Manager for Firewall installation”](#) on page 149.

- 16 To start the Event Collector and SESA Agent daemons, do one of the following:

- Reboot your system.
- Manually start the Event Collector and SESA Agent.
From a command line prompt on the log server, type:

```
/etc/init.d/sesagentd start
```

```
/etc/init.d/sefcollectord start
```

Upgrading from Symantec Event Manager for Firewall v1.0 to Symantec Event Manager for Security Gateways v2.0.1

If you are currently collecting events from v7.0.x Symantec security gateways or third-party security gateways, two upgrade paths are supported:

- Symantec Event Manager for Firewall v1.0 to Symantec Event Manager for Security Gateways (Group 1) v2.0.1
After upgrading, you can collect events from v7.0.x and v8.0 Symantec security gateways and third-party security gateways.
- Symantec Event Manager for Firewall v1.0 to Symantec Advanced Manager for Security Gateways (Group 1) v2.0.1
After upgrading, you can collect events from v7.0.x and v8.0 Symantec security gateways. In addition, you can manage the configurations of v8.0 Symantec security gateways using Symantec Advanced Manager v2.0.1.

This section describes the procedure to upgrade to Symantec Event Manager for Security Gateways (Group 1) v2.0.1. You can use the same procedure to upgrade to Symantec Advanced Manager for Security Gateways (Group 1) v2.0.1.

When you upgrade, you must uninstall the SESA integration components of Symantec Event Manager for Firewall v1.0.

You upgrade only the SESA integration components that are installed on the SESA Manager: you do not need to upgrade the Symantec Event Manager for Firewall components that are installed on remote log servers or third-party security gateways.

Note: If you are also upgrading your version of SESA, upgrade SESA after you uninstall Symantec Event Manager for Firewall v1.0 and before you install Symantec Event Manager for Security Gateways (Group 1) v2.0.1.

To upgrade from Symantec Event Manager for Firewall v1.0

- 1 Upgrade SESA to the latest patch level.
 For SESA patches, go to the Symantec Enterprise Security Architecture link on the Symantec Support Web site:
http://www.symantec.com/techsupp/enterprise/products/sesa/sesa_1.1/files.html
- 2 Stop event collection.
 On the remote log server on which the Event Collector for Firewall is installed, stop the SEF-SGS EventCollector Service and the SESA AgentStart service.
 See “Starting and stopping the Event Collector in Microsoft Windows” on page 144 and “Starting and stopping the Event Collector in Solaris” on page 145.
- 3 On the SESA Manager, save your v7.0.x Symantec security gateway events and third-party security gateway events using one of the following techniques:
 - Make a backup of the SESA DataStore.
 See the following Symantec Knowledge Base article for backup instructions:
<http://service1.symantec.com/SUPPORT/ent-gate.nsf/docid/2003042816055954>
 This article, “How to migrate a SESA DB2 DataStore to a different computer,” describes the backup and restore process.
 - Export and save events using SESA’s Firewall Event family of reports.
 To create a record of your events without keeping them active in the SESA DataStore, you can use the Export function on the Alerts or Events view tab. This lets you save the data in reports to an HTML file, PDF file, or CSV (Comma Separated Values) file.
- 4 Log off the SESA Console and ensure that no other security gateway managers are logged on to the SESA Console.
- 5 Uninstall the SESA integration components of the Symantec Event Manager for Firewall v1.0.
 Do the following:
 - On the SESA Manager, in a DOS window, navigate to the C:\SESA\UNINSTALL folder.
 - On the command line, type the following command:
`java -jar setup.jar -uninstall`
 This runs the Symantec Event Manager for Firewall SIPI installation in uninstall mode.

- Follow the SESA Installation Wizard prompts.
The information you are prompted for when you uninstall is the same as the information for installing. For a description of how to respond to the prompts, see [“Installing Symantec Event Manager for Security Gateways”](#) on page 76.
After you complete the wizard, the uninstall removes the Symantec Event Manager for Firewall event schemas from the SESA DataStore and SESA Directory, and unregisters Symantec Event Manager for Firewall.
- 6 Install Symantec Event Manager for Security Gateways (Group 1) v 2.0.1 or Symantec Advanced Manager for Security Gateways (Group 1) v 2.0.1.
See [“Installing Symantec Event Manager for Security Gateways”](#) on page 73 or [“Installing Symantec Advanced Manager for Security Gateways”](#) on page 61.
- 7 If you backed up the v7.0.x Symantec security gateway events and alerts from the SESA DataStore, restore them.
- 8 Restart event collection.

Configuring network interfaces and remote management hosts

After installing the Event Manager for Firewall and Event Collector for Symantec Security Gateways, you must edit the FirewallInformation.ini file, to specify system names for internal/external network interfaces and IP addresses for Remote Management Host computers.

- In Windows, the FirewallInformation.ini file is located in:
C:\Program Files\Symantec\FWEvent Manager\
KnowledgeBase\Firewalls\SEF\FirewallInformation.ini.
- In Solaris the FirewallInformation.ini file is located in:
/opt/Symantec/FWEventManager/KnowledgeBase/Firewalls/SEF/
FirewallInformation.ini.

To configure network interfaces and remote management host computers

- 1 Open the FirewallInformation.ini file in a text editor of your choice.

```
1,FirewallInformation,new,20,20,-1,F
CommunicationParameters,AlertDest,IM
InternalInterfaces
ExternalInterfaces
Proxies
RemoteManagementPorts,416,417,418
RemoteManagementHosts
```

- 2 In the InternalInterfaces row, add the name and IP address of each inside (internal) interface for the first firewall that the Event Collector for Symantec Security Gateways will monitor.

The format of this row is:

```
<InterfaceName1>,<IPAddress1>;<InterfaceName2>,<IPAddress2>;...
```

Enter the information for as many interfaces as necessary, using commas to separate the name and IP addresses for an interface, and semicolons to separate multiple interface name and address pairs.

If you are unsure of what to enter here, you can obtain a list of firewall interface names and IP addresses in one of the following ways:

- In Solaris or Linux environments, open the Symantec Raptor Management Console (SRMC), and expand **Symantec Enterprise Management >Base Components >Network interfaces**.
 - In a Windows environment, search a log file for 'srcif' and 'dstif' after passing network traffic.
- 3 In the ExternalInterfaces row, add the name and IP address of the outside (external) interface for the first firewall that the Event Collector for Symantec Security Gateways will monitor.
 - 4 In the Remote Management Hosts row, type the IP address for each Remote Management Host computer. Separate multiple IP addresses with commas. These are computers on which the Symantec Raptor Management Console (SRMC) or the Event Collector for Symantec Security Gateways are installed.

Customizing the SESA Agent's configuration

For the best performance and reliability, use the Configurations view tab of the SESA Console to change the parameters of the SESA Agent parameters that is installed on the log server to the settings in the following procedure.

Note: For information on all SESA Agent parameters and settings, see the chapter on configuring products in the *Symantec Enterprise Security Architecture Administrators Guide*.

Table 11-4 Recommended SESA Agent Settings

Parameter	Recommend ed setting	Description
Maximum queue size	9999 KB	When an application's queue reaches this size, any future log requests are refused.
App flush size	999 KB	Agent outbound data is sent to the SESA Manager whenever one of the three triggers is tripped. Note: This only applies to batch events; direct events are always sent as soon as possible.
App flush count	1000	
App flush time	60 seconds	
App spool size	1000 KB	Size in kilobytes of the Event Collector queue that the SESA Agent holds in memory when not able to send the normal queue to the SESA Manager. If the queue exceeds this size, and it still needs to grow, the queue is written to disk.

To edit SESA Agent parameters

- 1

In the SESA console, on the Configurations view tab, in the left pane, expand the SESA folder.
- 2

Expand SESA Agent Configuration.
- 3

On the Logging tab, change the parameters to the settings in [Table 11-4](#).
- 4

When you finish editing the configuration, select one of the following:

Apply

Save your changes and continue editing.

Reset

Cancel all of the changes that you have made on all of the tabs and reset the values to those that existed when you started editing.

- 5 When you are prompted to distribute the changes, select one of the following:
- Yes Immediately inform computers that are associated with the configuration of the changes. The computers receive a message that a new configuration is waiting.
 - No Inform computers of the changes at a later time, or the computers will pick up changes at the next scheduled configuration update interval.

When you distribute a configuration, the software of the target systems will retrieve their new configuration immediately.

Customizing the SESA Manager's configuration

To ensure the timely distribution of events, use the Configurations view tab of the SESA Console to change SESA Manager parameters to the settings described in the following procedure.

Note: For information on all SESA Manager parameters and settings, see the chapter on configuring products in the *Symantec Enterprise Security Architecture Administrators Guide*.

Table 11-5 Recommended SESA Manager settings

Parameter	Recommended setting	Description
Throttle server	0 seconds	Configures the minimum time between successive connections to a SESA Manager from a manager when sending data. If requests are made too frequently, they are rejected until the throttle interval has expired.
Throttle desktop	0 seconds	Minimum time between successive connections to a SESA Manager from a client when sending data. If requests are made too frequently, they will be rejected until the throttle interval has expired. This results in the generation of a hyperactive client event.

To edit SESA Manager parameters

- 1 In the SESA Console, on the Configurations view tab, in the left pane, expand the SESA folder.
- 2 Expand SESA Manager Configuration.
- 3 On the Throttle tab, change the parameters to the settings in [Table 11-5](#).
- 4 When you finish editing the configuration, select one of the following:

Apply	Save your changes and continue editing.
Reset	Cancel all of the changes that you have made on all of the tabs and reset the values to those that existed when you started editing.

- 5 When you are prompted to distribute the changes, select one of the following:

Yes	Immediately inform computers that are associated with the configuration of the changes. The computers receive a message that a new configuration is waiting.
No	Inform computers of the changes at a later time, or the computers will pick up changes at the next scheduled configuration update interval.

When you distribute a configuration, the software of the target systems retrieves their new configuration immediately.

Configuring Symantec Event Manager for Firewall to monitor multiple Symantec Security Gateways

Symantec Event Manager for Firewall is configured during installation to monitor the log file of a single Symantec security gateway. If your environment requires you to monitor more than one security gateway, you must change the settings of the `RaptorExpert.ini` and `SEFLogSensor.ini` files. Procedures for modifying both files are contained in this section.

See the section on Customizing the Symantec Event Manager for Firewall in the *Symantec Advanced Manager for Security Gateways (Group 1) V2.0.1* and *Symantec Event Manager for Security Gateways (Group 1) V2.0.1 Administrator's Guide* for detailed descriptions of the `RaptorExpert.ini` and `SEFLogSensor.ini` configuration files.

How the Event Collector for Symantec Security Gateways manages multiple log files

The Event Collector logs events from multiple security gateways by running a unique instance of the RemoteLog Utility for each security gateway that is being monitored.

To work properly, you must configure remote logging on the log server and on each Symantec security gateway to be monitored. Configure each log server and security gateway with the other's IP address and a shared password granting the log server permission to connect to the security gateway and obtain its log files.

See [“Remote Log utility”](#) on page 113.

Once Remote Logging has started, the Event Collector queries the log files, collects and formats events, and forwards them to the SESA Agent for logging to the SESA Manager.

The Event Collector uses sensors to read log files and report events from each monitored security gateway. The sensors are configured in the SEFLogSensor.ini and RaptorExpert.ini configuration files, which are built dynamically during installation.

They work together to define each firewall to be monitored.

- The SEFLogSensor.ini file defines attributes of a single security gateway. It contains parameters that identify the location of the security gateway, the source log file on the security gateway, the local log file to monitor, and whether you choose to archive log files.

To monitor more than one log file, you must create a unique SEFLogSensor.ini file *for each* security gateway, and change the following parameter settings: DeviceIP, LogToMonitor, SourceLogPath, AltLog, and optionally LogPath.

- The RaptorExpert.ini file includes a sensor property record that corresponds to each SEFLogSensor.ini file.
 After you create a unique SEFLogSensor.ini file for each security gateway, you must edit RaptorExpert.ini to add a sensor record that points to each sensor log file.

Configuring Symantec Event Manager for Firewall to monitor multiple log files

Follow these instructions to configure the Symantec Event Manager for Firewall to monitor log files from multiple Symantec security gateways.

To configure Event Manager for Firewall to monitor multiple log files:

1 In one of the following directories:

- In Microsoft Windows:

C:\Program Files\Symantec\FWEvent
Manager\KnowledgeBase\Firewalls\SEF\

- In Sun Solaris:

/opt/Symantec/FWEventManager/KnowledgeBase/Firewalls/SEF/

Make one copy of the SEFLogSensor.ini file for each security gateway to be monitored. Give each a unique name and store in the default directories.

Note: You can give additional sensor log files any name. For example, you can name them by appending a number to the end of each file, as follows: SEFLogSensor1.ini, SEFLogSensor2.ini, and so on.

The only requirement is that when you edit RaptorExpert.ini, you enter a sensor property record that corresponds to each unique sensor log file, beginning with SEFLogSensor.ini.

2 Open RaptorExpert.ini using a text editor.

```
ExportType:RaptorExpert;  
ComType:sesa;  
DEToSESAMapFile:../KnowledgeBase/Firewalls/SEF/  
DEToSesaMap.xml;  
SESAProductIF:3016;  
SesaSwFeatureId:30160102;  
SesaProductVersion:1.0;  
BaseRuleFile:../KnowledgeBase/Firewalls/SEF/SEF.kbt;  
LocatorFilePath:../Com;  
ListeningPort:0;  
BindAddress:127.0.0.1;  
InactiveSensorReportInterval:60;  
RemotelogutilPath:"/program files/raptor/firewall/bin/  
remotelogfile";  
Sensor:LogSensor ParameterFile:../KnowledgeBase/Firewalls/SEF/  
SEFLogSensor.ini MaxEventsToRead:1000 ReportInactivity:FALSE  
SampleRate:-1;
```

- 3
For each sensor log file that you created in step 2, do the following:
 - Make a copy of the sensor property record (the line beginning with "Sensor")
 - Paste it after the first sensor property record in RaptorExpert.ini.
 - Add the name of the new sensor log file to the sensor property record, as follows:

```
Sensor:LogSensor ParameterFile:../KnowledgeBase/Firewalls/SEF/ <sensor log file> MaxEventsToRead:1000
ReportInactivity:FALSE SampleRate:-1;
```

where <sensor log file> is the name of the new sensor log file. For example: SEFLogSensor1.ini.
Precede any line break that you add to the sensor property record with a space character. There must be a space at the end of each line before the last line in the file, which must end with a semi-colon.

- 4
Save and close the RaptorExpert.ini file.

- 5
Open each sensor log file, starting with SEFLogSensor.ini.

```
DeviceIP:10.1.1.5.8;
LogPath:"c:\raptor\firewall\bin/";
LogToMonitor:"logfile";
NameIsDynamic:False;
TranslationFile:"../KnowledgeBase/Firewall/SEF/SEF.trn";
SensorType:FirewallLogSensor;
MonitorInRealTime:True
InitialReadPolicy:Beginning;
EndofRecordMarker:0x0A;
AltLog:"logfile1";
SrcLogPath:"logfile";
ArchiveLogs:0;
```

- 6
Change the following parameter settings:

DeviceIP	Type the IP address of the firewall being monitored.
LogToMonitor	Type the name you chose during installation for the initial (local) log file. This will be stored in the LogPath directory.
SrcLogPath	Type the name of the log file on the firewall. It is the file name parameter that is passed to remotelogfile.
AltLog	Type the file name of the alternate log file, chosen during installation, when the option to archive log files is disabled. Event records are logged dynamically between the two files identified in LogToMonitor and AltLog.
LogPath (optional)	Type the pathname of the local directory (with optional drive identifier for Windows) where copies of the log files will be stored for this sensor.

- 7 Save and close each sensor log file.
- 8 For the changes to take effect, restart the Event Collector for Symantec Security Gateways.
See [“Event Collector for Symantec Security Gateways service/daemon”](#) on page 144.

Event Collector for Symantec Security Gateways service/daemon

The Event Collector for Symantec Security Gateways runs as a service (in Microsoft Windows) or a daemon (in Solaris) on the computer on which it is installed.

In both environments, the SESA Agent must be running before the Event Collector can successfully initialize. If the Event Collector is started before the SESA Agent or if the SESA Agent is still initializing when the Event Collector is started, the Event Collector tries to connect to the SESA Agent for 60 seconds before closing.

Refer to the appropriate section below for instructions on starting and stopping the Event Collector in both the Microsoft Windows and Solaris environments.

Starting and stopping the Event Collector in Microsoft Windows

In Microsoft Windows, the installation process installs the Event Collector as a service. The Event Collector is accessible through the Services control panel applet and through the Add/Remove Programs control panel applet.

The installation also registers the SESA Agent as a service, which is accessible through the Services control panel.

To start and stop the Event Collector, you start and stop the service as necessary, in one of the following ways:

- Restarting the log server computer.
- Using the Windows Services control panel.

Procedures for starting and stopping services in Microsoft Windows depend on the version of Windows that is installed. The following procedure is for Windows 2000 or Windows XP.

To start or stop a service from the Windows Services dialog box

- 1 On the computer on which you installed the Event Collector, on the Windows taskbar, click **Start > Settings > Control Panel**.
- 2 In the Control Panel window, double-click **Administrative Tools**.
- 3 In the Administrative Tools window, double-click **Services**.
- 4 In the Services dialog box, right-click the SEF-SGS Event Collector service.
- 5 Click **Start** or **Stop**.

Starting and stopping the Event Collector in Solaris

In Solaris, the Event Collector is installed and runs automatically as a daemon. You can also manually start and stop the Event Collector daemon, if necessary.

From a command line prompt on the log server, you start and stop the Event Collector daemon using two different commands.

To start and stop the Event Collector in Solaris

- 1 To start the Event Collector, type the following command:
`# /etc/init.d/sefcollectord start`
- 2 To stop the Event Collector, type the following command:
`# /etc/init.d/sefcollectord stop`

Managing disk space for log files

Symantec Event Manager for Firewall provides two options for managing disk space for log files:

- Archive log files
- Dynamically save event records between two active log files (no archiving occurs)

You decide how log files are managed when you install Event Manager for Firewall. See [“Installing Symantec Event Manager for Firewall”](#) on page 128.

Archiving log files

When you install the Event Collector for Symantec Security Gateways, you can specify that log files are archived. In the Logfile Information panel of the Install Wizard, you specify the directory in which log files are stored on the log server, and a base name under which log files are stored, and you specify that you want to archive log files.

Log file archival takes place as follows:

- When the Event Collector is started, event records are retrieved from the security gateway and stored under the base log file name in the directory you specified.
- When the current log file reaches a maximum size of 50,000 events, it is renamed, with the year, month, and day as a suffix. As subsequent log files are archived, numerical designations are appended to the end of each file name.
For example, when the designated name is logfile, archived log files are named as follows:
logfile.20030331-1, logfile. 20030331-2, and so forth
- Each time a log file is archived, a new log file is automatically created on the log server, using the designated name and directory.

If you did not select to archive log files during installation, but later want to start a log file archive, do the following:

- In the SEFLogSensor.ini file, change the value of the ArchiveLogs row to 1.
ArchiveLogs=1
- Delete all previously stored log files
- Restart the Event Collector.

Saving log files dynamically

If you do not want to archive log files, you can save them dynamically. During installation, on the Logfile Information panel, you specify the initial log file name on the log server, and an alternate name.

When the Event Collector starts, both the initial and alternate log files are used together to manage events. The initial log file is filled first, until it reaches a maximum size of 50,000 event records. Events are then saved in the alternate log file, until it reaches 50,000 event records.

At this point, the initial log file is purged and events are logged to that file again until it reaches 50,000 records. When the initial log file is full, the alternate log file is then purged and events are recorded there once again.

Uninstalling the Event Collector for Symantec Security Gateways

Uninstalling the Event Collector removes the collector itself and also removes the SESA Agent if no other products on the log server are using it.

Refer to the appropriate section below for instructions on uninstalling the Event Collector in both the Microsoft Windows and Solaris environments.

Uninstalling the Event Collector in Microsoft Windows

You can uninstall the Event Collector using the Microsoft Windows Add/Remove Programs feature.

Note: After you uninstall, the Symantec Event Collector service (and the SESAAgentStart service, if the SESA Agent is uninstalled) is removed from the Windows Services control panel.

To uninstall the Event Collector in Microsoft Windows

- 1 On the computer on which the Event Collector is installed, on the Windows taskbar, click **Start > Settings > Control Panel**.
- 2 In the Control Panel window, double-click **Add/Remove Programs**.
- 3 In the Add/Remove Programs dialog box, click **Symantec Event Manager for Firewall**, and then click **Remove**.
- 4 When you are prompted to remove Symantec Event Manager for Firewall from your computer, click **Yes**.

Symantec Event Collector is removed from the Add/Remove Programs dialog box, indicating that the Event Collector is removed.

Uninstalling the Event Collector in Solaris

You uninstall the Event Collector in Solaris manually from the command line of the log server.

To uninstall the Event Collector in Solaris

- 1 To delete the /opt/Symantec directory, type the following command:

```
rm -rf /opt/Symantec
```
- 2 To delete the /etc/symantec directory, type the following command:

```
rm -rf /etc/symantec
```

- 3 To change directories, type the following command:
`cd /etc/init.d`
- 4 To delete the sesagentd file, type the following command:
`rm sesagentd`
- 5 To delete the sefcollectord file, type the following command:
`rm sefcollectord`

Verifying Symantec Event Manager for Firewall installation

This chapter includes the following topics:

- [Verifying that the service or daemon has started](#)
- [Examining SESA Agent logs](#)
- [Verifying Symantec Security Gateway appears in the SESA Console](#)
- [Troubleshooting the Symantec Event Manager for Firewall installation](#)

Note: The topics discussed in this chapter apply to Symantec Event Manager for Firewall only.

For information on Symantec Event Manager for Security Gateways, see [“Event management concepts”](#) on page 41.

Verifying that the service or daemon has started

After you install Symantec Event Manager for Firewall, a key indication that installation was successful is if the service (in Microsoft Windows) or daemon (in Sun Solaris 8 or 9) has started.

To verify that the service or daemon has started

You can verify if the service has started on Microsoft Windows, or if the daemon started on Solaris.

To verify that services have started (Microsoft Windows)

- 1 On the log server, select **Start > Settings > Control Panel > Administrative Tools > Services**.
- 2 In the Services window, verify that the following services are running:
 - Symantec Event Collector for SEF-SGS Event Collector
 - SESA AgentStart Service

To verify that the daemon has started (Solaris)

- ◆ To verify that the daemon has started, from a command prompt on the log server, type the following command:

```
ps -ef | grep agentd
ps -ef | grep RaptorExpert-run.sh
```

Examining SESA Agent logs

Examining the SESA Agent logs can help you to determine if both successfully started.

To examine the SESA Agent logs

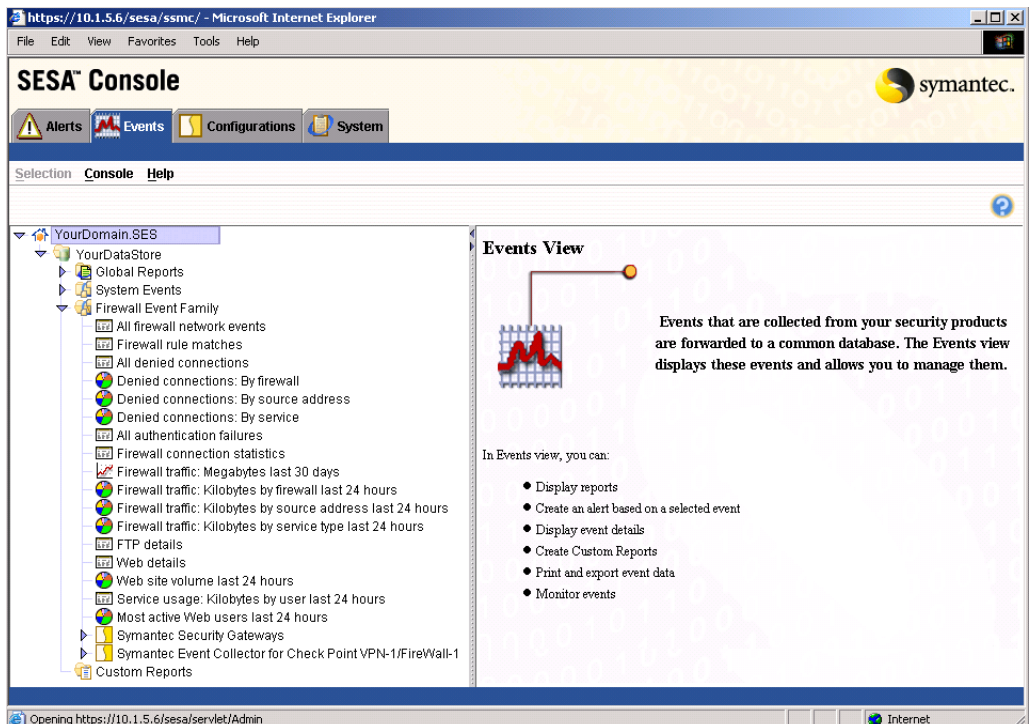
- 1 On the log server, navigate to the SESA Agent log.
 - In Microsoft Windows, the default location is:
C:\Program Files\Symantec\SESA\Agent\sesa-agent.log.
 - In Sun Solaris 8 or 9, the default location is:
/opt/Symantec/sesa/sesa-agent.log.
- 2 You should see the following entry:
SESA Agent ***Bootstrap successful
- 3 In Microsoft Windows only, select **Start > Settings > Control Panel > Administrative Tools > Event Viewer**.
- 4 Click **Application Log**.
- 5 Examine the log. You should see the following log entry:
The service was started

Verifying Symantec Security Gateway appears in the SESA Console

Check to verify that Symantec Security Gateway appears in the Configurations view tab of the SESA Console.

To verify that Symantec Security Gateway displays in the SESA Console

- 1 On the SESA Manager computer, on the Windows taskbar, click **Start > Programs > Symantec Enterprise Security > SESA Console**.
 If you are not working directly on the SESA Manager computer, to connect to the SESA Console, in a browser window type the URL of the SESA Manager.
- 2 Log on to the SESA Console using a SESA user account with sufficient rights to view SESA events.
 The SESA user must belong to a role that has rights to the SESA-enabled Symantec Event Collector product.
- 3 On the Event view tab, expand your domain, and then expand **SESA DataStore > Firewall Event Family**



- 4 Under Firewall Event Family, verify that the Symantec Security Gateways folder is listed.
- 5 On the Configurations view tab, expand Symantec Security Gateway.
- 6 Verify that the following item is listed:
 - Symantec Security Gateway

For more information on reports and views, see the *Symantec Enterprise Security Architecture Administrators Guide*.

Troubleshooting the Symantec Event Manager for Firewall installation

If you are not receiving security gateway events after installing the Event Manager for Firewall, perform the following procedures to confirm operation:

- [Verifying the SESA Manager address and port.](#)
- [Verifying remote logging operation for Symantec security gateways.](#)
- [Verifying Event Collector operation](#)

Note: When first installed, the Event Manager for Firewall is configured (by default) to generate all but statistical events. This helps to ensure the best possible performance.

To enable statistical event reporting, see the section on customizing the Symantec Event Manager for Firewall in the *Symantec Advanced Manager for Security Gateways (Group 1) V2.0.1 and Symantec Event Manager for Security Gateways (Group 1) V2.0.1 Administrator's Guide*.

Verifying the SESA Manager address and port

Verify that you specified the correct SESA Manager IP address (or host name) and the correct number for the SESA secure directory port when you ran the SESA Integration Wizards.

To verify the SESA Manager address and port

- 1 On the log server computer, at the command prompt, change to one of the following directories:
 - In Microsoft Windows:
C:\Program Files\Symantec\SESA\Agent
 - In Sun Solaris 8 or 9:
/opt/Symantec/sesa
- 2 In a text editor, open the Configprovider.cfg file.
- 3 Verify that the following options contain the correct settings for the SESA Manager to which you want to send security gateway events:

mgmtServer	Should contain the IP address of the SESA Manager
mgmtPort	Should contain the port that you chose for secure data. Default: 443

Verifying remote logging operation for Symantec security gateways

To verify that the remote logging feature is working properly, view a remote log file for a Symantec security gateway from a command prompt on the log server.

To verify remote logging operation

- ◆ To verify that remote logging is operating, type the following command:

```
remotelogfile <IP address of the security gateway> logfile
```

If remote logging is configured correctly on the security gateway and the log server, you should see the text of the remote log file scroll rapidly by on the log server's monitor.

Verifying Event Collector operation

You can verify Event Collector operation by confirming that the proper services are running and that there are no error messages in the application log file.

To verify Event Collector operation

You can verify Event Collector in Microsoft Windows or Sun Solaris 8 or 9.

To verify Event Collector operation in Microsoft Windows

- 1 On the log server, select **Start > Settings > Control Panel > Administrative Tools > Services**.
- 2 In the Services window, verify that the following services are running:
 - Symantec Event Collector for SEF-SGS Event Collector
 - SESA AgentStart Service
- 3 Close the Services window.
- 4 Select **Event Viewer**.
- 5 In the Event Viewer, examine the Application Log for failure events from the Symantec Event Collector for SEF-SGS Event Collector.
If you see only success events, the problem most likely exists elsewhere.
- 6 Close the Event Viewer and the Administrative Tools windows.

To verify Event Collector operation in Sun Solaris 8 or 9

- ◆ To verify Event Collector operation, from the command line on the log server, type the following commands:

```
ps -ef | grep RaptorExpert-run.sh
ps -ef | grep agentd
```

Licensing

This chapter includes the following topics:

- [Symantec Advanced Manager and Symantec Event Manager licensing](#)
- [SYMANTEC SOFTWARE LICENSE AGREEMENT](#)

Symantec Advanced Manager and Symantec Event Manager licensing

Symantec Advanced Manager for Security Gateways (Group 1) v2.0.1 and Symantec Event Manager for Security Gateways (Group 1) v2.0.1 are optional products that integrate with Symantec Enterprise Security Architecture to provide enterprise-wide scalable management, event logging, alerting and reporting.

Licensing is by the number of security gateways managed or sending events to the SESA Manager. The minimum license provides services for up to five security gateways. A Symantec Advanced Manager license includes a license for Symantec Event Manager. You can purchase Symantec Event Manager licenses separately, although if Symantec Advanced Manager is licensed, you must have the same number of licenses for Symantec Event Manager. Licenses are available in 5, 25, 100, and unlimited increments.

SYMANTEC SOFTWARE LICENSE AGREEMENT

SYMANTEC CORPORATION AND/OR ITS SUBSIDIARIES ("SYMANTEC") IS WILLING TO LICENSE THE SOFTWARE TO YOU AS AN INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING THE SOFTWARE (REFERENCED BELOW AS "YOU" OR "YOUR") ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT. READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE USING THE SOFTWARE. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU AND THE LICENSOR. BY OPENING THIS PACKAGE, BREAKING THE SEAL, CLICKING THE "AGREE" OR "YES" BUTTON OR OTHERWISE INDICATING ASSENT ELECTRONICALLY, OR LOADING THE SOFTWARE, YOU AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, CLICK THE "I DO NOT AGREE" OR "NO" BUTTON OR OTHERWISE INDICATE REFUSAL AND MAKE NO FURTHER USE OF THE SOFTWARE.

1. LICENSE:

The software and documentation that accompanies this license (collectively the "Software") is the proprietary property of Symantec or its licensors and is protected by copyright law. While Symantec continues to own the Software, You will have certain rights to use the Software after Your acceptance of this license. This license governs any releases, revisions, or enhancements to the Software that the Licensor may furnish to You. Except as may be modified by an applicable Symantec license certificate, license coupon, or license key (each a "License Module") that accompanies, precedes, or follows this license, and as may be further defined in the user documentation accompanying the Software, Your rights and obligations with respect to the use of this Software are as follows.

YOU MAY:

- A. use the number of copies of the Software as have been licensed to You by Symantec under a License Module. If the Software is part of a suite containing multiple Software titles, the number of copies You may use may not exceed the aggregate number of copies indicated in the License Module, as calculated by any combination of licensed Software titles. Your License Module shall constitute proof of Your right to make such copies. If no License Module accompanies, precedes, or follows this license, You may make one copy of the Software You are authorized to use on a single computer;
- B. make one copy of the Software for archival purposes, or copy the Software onto the hard disk of Your computer and retain the original for archival purposes;
- C. use the Software on a network, provided that You have a licensed copy of the Software for each computer that can access the Software over that network
- D. use the Software in accordance with any written agreement between You and Symantec; and
- E. after written consent from Symantec, transfer the Software on a permanent basis to another person or entity, provided that You retain no copies of the Software and the transferee agrees in writing to the terms of this license.

YOU MAY NOT:

- A. copy the printed documentation that accompanies the Software;
- B. sublicense, rent, or lease any portion of the Software; reverse engineer, decompile, disassemble, modify, translate, make any attempt to discover the source code of the Software, or create derivative works from the Software;
- C. use the Software as part of a facility management, timesharing, service provider, or service bureau arrangement;
- D. use a previous version or copy of the Software after You have received a disk replacement set or an upgraded version. Upon upgrading the Software, all copies of the prior version must be destroyed;
- E. use a later version of the Software than is provided herewith unless You have purchased corresponding maintenance and/or upgrade insurance or have otherwise separately acquired the right to use such later version;
- F. use, if You received the software distributed on media containing multiple Symantec products, any Symantec software on the media for which You have not received permission in a License Module; nor
- G. use the Software in any manner not authorized by this license.

2. CONTENT UPDATES:

Certain Software utilize content that is updated from time to time (including but not limited to the following Software: antivirus software utilize updated virus definitions; content filtering software utilize updated URL lists; some firewall software utilize updated firewall rules; and vulnerability assessment products utilize updated

vulnerability data; these updates are collectively referred to as "Content Updates"). You shall have the right to obtain Content Updates for any period for which You have purchased maintenance, except for those Content Updates that Symantec elects to make available by separate paid subscription, or for any period for which You have otherwise separately acquired the right to obtain Content Updates. Symantec reserves the right to designate specified Content Updates as requiring purchase of a separate subscription at any time and without notice to You; provided, however, that if You purchase maintenance hereunder that includes particular Content Updates on the date of purchase, You will not have to pay an additional fee to continue receiving such Content Updates through the term of such maintenance even if Symantec designates such Content Updates as requiring separate purchase. This License does not otherwise permit the licensee to obtain and use Content Updates.

3. LIMITED WARRANTY:

Symantec warrants that the media on which the Software is distributed will be free from defects for a period of sixty (60) days from the date of delivery of the Software to You. Your sole remedy in the event of a breach of this warranty will be that Symantec will, at its option, replace any defective media returned to Symantec within the warranty period or refund the money You paid for the Software. Symantec does not warrant that the Software will meet Your requirements or that operation of the Software will be uninterrupted or that the Software will be error-free.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE ABOVE WARRANTY IS EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS, WHICH VARY FROM STATE TO STATE AND COUNTRY TO COUNTRY.

4. DISCLAIMER OF DAMAGES:

SOME STATES AND COUNTRIES, INCLUDING MEMBER COUNTRIES OF THE EUROPEAN ECONOMIC AREA, DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE BELOW LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW AND REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE, IN NO EVENT WILL SYMANTEC BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INDIRECT, OR SIMILAR DAMAGES, INCLUDING ANY LOST PROFITS OR LOST DATA ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE EVEN IF SYMANTEC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

IN NO CASE SHALL SYMANTEC'S LIABILITY EXCEED THE PURCHASE PRICE FOR THE SOFTWARE. The disclaimers and limitations set forth above will apply regardless of whether or not You accept the Software.

5. U.S. GOVERNMENT RESTRICTED RIGHTS:

RESTRICTED RIGHTS LEGEND. All Symantec products and documentation are commercial in nature. The software and software documentation are "Commercial Items," as that term is defined in 48 C.F.R. section 2.101, consisting of "Commercial Computer Software" and "Commercial Computer Software Documentation," as such terms are defined in 48 C.F.R. section 252.227-7014(a)(5) and 48 C.F.R. section 252.227-7014(a)(1), and used in 48 C.F.R. section 12.212 and 48 C.F.R. section 227.7202, as applicable. Consistent with 48 C.F.R. section 12.212, 48 C.F.R. section 252.227-7015, 48 C.F.R. section 227.7202 through 227.7202-4, 48 C.F.R. section 52.227-14, and other relevant sections of the Code of Federal Regulations, as applicable, Symantec's computer software and computer software documentation are licensed to United States Government end users with only those rights as granted to all other end users, according to the terms and conditions contained in this license agreement. Manufacturer is Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014, United States of America.

6. EXPORT REGULATION:

Export or re-export of this Software is governed by the laws and regulations of the United States and import laws and regulations of certain other countries. Export or re-export of the Software to any entity not authorized by, or that is specified by, the United States Federal Government is strictly prohibited.

7. GENERAL:

If You are located in North America or Latin America, this Agreement will be governed by the laws of the State of California, United States of America. Otherwise, this Agreement will be governed by the laws of England and Wales. This Agreement and any related License Module is the entire agreement between You and Symantec relating to the Software and: (i) supersedes all prior or contemporaneous oral or written communications, proposals, and

representations with respect to its subject matter; and (ii) prevails over any conflicting or additional terms of any quote, order, acknowledgment, or similar communications between the parties. This Agreement shall terminate upon Your breach of any term contained herein and You shall cease use of and destroy all copies of the Software. The disclaimers of warranties and damages and limitations on liability shall survive termination. Software and documentation is delivered Ex Works California, U.S.A. or Dublin, Ireland respectively (ICC INCOTERMS 2000). This Agreement may only be modified by a License Module that accompanies this license or by a written document that has been signed by both You and Symantec. Should You have any questions concerning this Agreement, or if You desire to contact Symantec for any reason, please write to: (i) Symantec Customer Service, 555 International Way, Springfield, OR 97477, U.S.A., (ii) Symantec Authorized Service Center, Postbus 1029, 3600 BA Maarssen, The Netherlands, or (iii) Symantec Customer Service, 1 Julius Ave, North Ryde, NSW 2113, Australia.

Index

A

- activation, of security gateway configurations 32
- address, verifying for SESA Manager 153
- Advanced Manager. *See* Symantec Advanced Manager
- agent settings file, verifying 153
- alerts
 - creating 47
 - description 24
- antivirus event family 47
- Apache Tomcat memory usage
 - increasing 69
 - lowering 70
 - tuning 69
- association, of configurations with security gateways 31

B

- back up
 - SESA DataStore 68, 134
 - SESA Directory 68

C

- CD-ROM contents
 - Symantec Advanced Manager for Security Gateways 62
 - Symantec Event Manager for Security Gateways 74
- CD-ROMs, replacing 18
- clientrempass 116
- clusters, joining SESA 94, 95
- configuration management roles 23
- configurations
 - activation 32
 - associating with security gateways 31
 - chaining 36
 - components 30
 - exporting 39
 - inheriting 38, 39
 - revision management 31

- configurations (cont.)
 - sharing 37, 38
 - validating 32, 36
- connectivity
 - testing between remote log server and SESA Manager 123
- content filtering event family 47

D

- Default organizational unit 22
- disk space
 - managing for log files (Symantec Event Manager for Firewall) 145
 - SESA DataStore 123
- Domain Administrator role 24

E

- Event Collector
 - overview 111
- Event Collector (Symantec Event Manager for Firewall) 111
 - daemon 144, 150
 - overview 110, 111
 - service 144, 150
 - starting and stopping
 - in Micorsoft Windows 144
 - in Sun Solaris 8 or 9 145
- event gating 45
- event management
 - concepts 41
 - examples 42
 - multiple security gateways 43
 - single security gateway 42
 - legacy security gateways 45
 - roles 23
 - single security gateway 42
- Event Manager for Firewall *See* Symantec Event Manager for Firewall
- Event Manager for Security Gateways. *See* Symantec Event Manager for Security Gateways

events

- controlling from local security gateway 45
- logging 24
- viewing reports 24, 46

F

Firewall Event Family reports

- description 46
- viewing 151

firewall events, mapping to SESA 111

I

installation

- Java Runtime 127
- options 56
- Symantec Advanced Manager for Security Gateways 64
- Symantec Event Manager for Firewall SESA Agent 128
- Symantec Event Manager for Security Gateways 76

J

Java Runtime Environment, installing 127

Join SESA Wizard 83

- options 87
- tasks performed 84

joining SESA

- options 55

L

legacy event management 45

license

- Symantec Advanced Manager for Security Gateways 155
- Symantec Event Manager for Security Gateways 155

local security gateways, specifying events logged to SESA 45

location settings

- associating with security gateways 31
- configuring in SESA 30
- inheriting 38
- one-to-many relationship 37
- sharing 38

log files (Symantec Event Manager for Firewall)

- archiving 145
- disk space management 145
- multiple log files
 - configuring for 142
 - managing 141
 - saving dynamically 146
- SESA Agent 150
- viewing 150
- viewing Application Log 154
- log server. *See* remote log server
- logging events 24

M

Managers organizational unit 22

memory usage, Apache Tomcat

- increasing 69
- lowering 70
- tuning 69

message queue limits, SESA Agent 111

N

network

- interfaces, configuring 136
- intrusion event family 47

notifications

- creating 47
- description 24

O

organizational units

- adding security gateway machines 21
- associating configurations 38
- creating 38
- Default organizational unit 22
- description 21
- Managers organizational unit 22
- managing multiple security gateways 32
- moving security gateways 39

overview

- Event Collector 111

P

- planning
 - example 52
 - integration starting point 54
- policies
 - associating with security gateways 31
 - configuring in SESA 30
 - inheriting 38
 - one-to-many relationship 37
 - sharing 35, 37, 38
- port, verifying for SESA Manager 153
- prerequisites
 - Symantec Advanced Manager for Security Gateways 51
 - Symantec Event Manager for Security Gateways 51

R

- registry, editing for Apache Tomcat memory tuning 70
- remote log server
 - SESA Manager connection 123
 - system requirements 124
- remote log server (Symantec Event Manager for Firewall)
 - configuring 116
 - connectivity to SESA Manager 123
 - installing
 - Remote Log utility 116
 - SESA Agent 128
- Remote Log utility
 - installation 116
- remote logging (Symantec Event Manager for Firewall) 113
 - enabling 114
 - verification 118, 153
- remote management hosts
 - configuring 136
- removing. *See* uninstalling
- Rempass option 117
- report families
 - antivirus event 47
 - content filtering event 47
 - firewall events 46
 - network intrusion event 47
 - security gateways (group 1) 47
 - sensitive content filtering event 47

reports

- antivirus event family 47
- content filtering event family 47
- description 25
- Firewall Event Family 46
- network intrusion event family 47
- security gateways (group 1) 47
- sensitive content filtering event family 47
- viewing 46
- viewing in SESA Console 67, 79, 151

roles

- configuration management 23
- defined in SESA 23
- event management 23

S

- security gateways (group 1), report families 47
- sensitive content filtering event family 47
- SESA
 - administrative features 21
 - alert notifications 24
 - components 19
 - description 19
 - event management
 - features 24
 - roles 23
 - Foundation Pack 15, 51
 - integration components 14, 110
 - joining 83
 - cluster members 94, 95
 - exporting local configuration 88
 - for event management 99
 - gathering connection information 86
 - importing configurations 91
 - options 87
 - preparation 84, 85
 - troubleshooting 100
 - network sizing requirements (Symantec Event Manager for Firewall) 125
 - organizational units 21
 - planning integration 49
 - reports 25
 - returning to local management 101
 - permanently 102
 - temporarily 102
 - roles 23
 - users 23

SESA Agent

- customizing (Symantec Event Manager for Firewall) 138
- description 20
- installing for Symantec Event Manager for Firewall
 - on Microsoft Windows 128
 - on Sun Solaris 8 or 9 132
- log 150
- message queue limits 111

SESA Console

- description 20
- logging on 67, 79, 100
- viewing
 - Firewall Event Family 151
 - Symantec Advanced Manager for Security Gateway logs 67
 - Symantec Event Manager for Security Gateway logs 79

SESA DataStore

- backing up 68, 134
- description 20
- system requirements (Symantec Event Manager for Firewall) 123

SESA Directory

- backing up 68
- description 20

SESA Domain Administrator 24**SESA Domain Administrator role 24****SESA Event Collector, third-party products 20****SESA Manager**

- address and port verification 153
- connectivity to remote log server (Symantec Event Manager for Firewall) 123
- customizing (Symantec Event Manager for Firewall) 139
- description 20
- remote log server connection 123
- system requirements 123
- system requirements (Symantec Event Manager for Firewall) 123

shared configurations, validation 36**software requirements**

- Symantec Advanced Manager for Security Gateways 51
- Symantec Event Manager for Security Gateways 51

Symantec Advanced Manager for Security Gateways

- CD-ROM contents 62
- description 15
- examples
 - multiple security gateway configuration 33
 - single security gateway configuration 28

features 16**increasing Apache Tomcat memory usage 69****installation**

- options 56
- procedure 64
- required information 63
- verification 67

joining SESA 91, 95

- cluster members 94
- event management 99
- exporting local configuration 88

leaving SESA management 101**license 155****lowering Apache Tomcat memory usage 70****management advantages 27****planning for integration 49****preparing to install 63****products supported 14****returning to local management**

- permanently 102
- temporarily 102

tuning Apache Tomcat memory usage 69**uninstalling 71****upgrading 68****using organizational units 32****viewing logs in SESA Console 67****Symantec Enterprise Security Architecture. *See* SESA****Symantec Event Manager for Firewall**

- archiving log files 145
- components 120
- daemon
 - verifying on Microsoft Windows 150
- data collection 109, 110, 121
- description 17, 108
- Event Collector 111
 - daemon 144
 - overview 110, 111
 - service 144, 150

Event Collector overview 111**Event Collector service 150****how events are reported 17**

Symantec Event Manager for Firewall (cont.)

- installation
 - preparation 122, 125
 - procedure 128
 - SESA integration components 126
 - troubleshooting 152
 - verification 149
- mapping firewall events to SESA 111
- monitoring multiple security gateways 140
- multiple log files
 - configuring for 142
 - managing 141
- network interfaces, configuring 136
- overview 108
- remote log server configuration 116
- Remote Log utility 113
- remote management hosts, configuring 136
- requirements 123
- services, verifying on Microsoft Windows 150
- SESA Agent
 - customizing 138
 - log 150
 - message queue limits 111
- SESA DataStore system requirements 123
- SESA integration components 110
- SESA Manager, customizing 139
- supported products 108
- system requirements
 - network sizing 125
 - remote log server 124
- uninstalling 147
- upgrading
 - to Symantec Advanced Manager for Security Gateways v2.0.1 134
 - to Symantec Event Manager for Security Gateways v2.0.1 134
- verifying Event Collector operation 154
- viewing in SESA Console 151
- viewing log files 150

Symantec Event Manager for Security Gateways

- CD-ROM contents 74
- description 16
- event reporting 17
- installation
 - options 56
 - procedure 76
 - required information 75
 - verification 79
- joining SESA 99

Symantec Event Manager for Security Gateways (cont.)

- leaving SESA management 101
- license 155
- planning for integration 49
- preparing to install 75
- products supported 14
- returning to local management
 - permanently 102
 - temporarily 102
- uninstalling 80
- upgrading
 - to Symantec Advanced Manager for Security Gateways 68
 - to v2.0.1 80
 - viewing logs in SESA Console 79
- system requirements 51
- SESA Manager 123
- Symantec Event Manager for Firewall
 - remote log server 124
 - SESA DataStore 123
 - SESA Manager 123
- System Setup Wizard 85

T

troubleshooting, Symantec Event Manager for Firewall installation 152

U

uninstalling

- Event Collector
 - Microsoft Windows 147
 - Sun Solaris 8 or 9 147
- Event Manager for Firewall 147
- Symantec Advanced Manager for Security Gateways 71
- Symantec Event Manager for Security Gateways 80

upgrading

- Symantec Advanced Manager for Security Gateways 68
- Symantec Event Manager for Firewall 134
- Symantec Event Manager for Security Gateways 68, 80

users, defined in SESA 23

utilities, Remote Log 113

V

validation, of configurations 32, 36

verification

 installation

 Symantec Advanced Manager for Security
 Gateways 67

 Symantec Event Manager for
 Firewall 149, 151

 Symantec Event Manager for Security
 Gateways 79

remote logging operation (Symantec Event
Manager for Firewall) 118, 153

service or daemon has started 149

SESA Manager address and port 153

Symantec Event Manager for Firewall
Event Collector operation 154

W

wizards

Join SESA Wizard 83

SESA Integration Wizard

 Symantec Advanced Manager for Security
 Gateways 64

 Symantec Event Manager for Firewall 120

 Symantec Event Manager for Security
 Gateways 76

Symantec Event Manager for Firewall

 InstallShield Wizard 120

System Setup Wizard 85